SOPHOS

Security made simple.

Sophos Mobile Control
Administratorhandbuch

Produktversion: 5
Stand: April 2015

Inhalt

1 Über Sophos Mobile Control....5
1.1 Sophos Mobile Control als lokale Installation und "as a Service"....5
1.2 Einleitung....6
2 Über die Sophos Mobile Control Web-Konsole....8
2.1 Voraussetzungen....8
2.2 Web-Konsolen-Benutzer....9
3 Wichtige Schritte für das Management von Geräten mit der Web-Konsole....10
4 Anmelden an der Sophos Mobile Control Web-Konsole....11
4.1 Erste Anmeldung....11
4.2 Anmeldung....11
4.3 Ändern Ihres Kennworts....11
4.4 Kennwort-Recovery....12
4.5 Abmelden....12
5 Die Benutzeroberfläche der Web-Konsole....13
6 Dashboard....14
7 Reports....15
8 Aufträge....16
8.1 Überwachen von Aufträgen in der Web-Konsole....16
9 Allgemeine Einstellungen....19
9.1 Persönliche Einstellungen....19
9.2 Kennwortrichtlinien....19
9.3 iOS-Client....20
9.4 Windows Phone-Client....20
9.5 E-Mail-Konfiguration....21
9.6 Technischer Kontakt....21
10 Konfigurieren der Benutzung des Self Service Portal für Endbenutzer....22
10.1 Erstellen von Self Service Portal Gruppen mit der internen Benutzerverwaltung....22
10.2 Konfigurieren von Self Service Portal Einstellungen....23
10.3 Verwalten von Self Service Portal Benutzern....26
11 Systemeinstellungen....31
11.1 Überprüfen Ihrer Lizenzen....31
11.2 Hochladen des Apple Push Notification Keystore....31
11.3 Konfigurieren eines VPP-Service-Token (sToken)....32
11.4 Konfigurieren von SCEP für iOS-Geräte....33

11.5 Konfigurieren des Benutzerverzeichnisses....34
11.6 Samsung Knox-Lizenz....34
12 Konfigurieren von Geräterichtlinien....35
12.1 Verfügbare Geräterichtlinien....36
12.2 Zuweisen von Geräterichtlinien zu Gerätegruppen....39
12.3 Compliance-Prüfung bei Geräten....39
13 Hinzufügen von Geräten zu Sophos Mobile Control....40
13.1 Erstellen von Gerätegruppen....40
13.2 Erstellen eines neuen Geräts....41
13.3 Duplizieren eines Geräts....41
13.4 Importieren von Geräten....42
14 Samsung Knox-Unterstützung....43
15 Mit Profilen arbeiten....44
15.1 Erstellen von Geräteprofilen für Android-Geräte....44
15.2 Erstellen von Container-Profilen für Android-Geräte....61
15.3 Erstellen von Profilen für iOS-Geräte....66
15.4 Anlegen von Windows Phone 8-Geräten....95
15.5 Platzhalter für Profile....101
15.6 Übertragen von Apple iOS-, Android- oder Windows Mobile-Profilen....102
15.7 Übertragen von Windows Phone 8-Profilen....102
15.8 Herunterladen von iOS-, Android- und Windows Phone 8-Profilen aus der Web-Konsole....103
16 Mit Auftragspaketen arbeiten....104
16.1 Erstellen von Auftragspaketen....104
16.2 Duplizieren von Auftragspaketen....105
16.3 Übertragen von Auftragspaketen an einzelne Geräte oder Gerätegruppen....105
17 Mit Apps arbeiten....106
17.1 Hochladen von Apps zur Web-Konsole....106
17.2 Anlegen von Links zu Apps....107
17.3 Verwaltung von mit dem Apple Volume Purchase Program erworbenen Apps....108
17.4 Installation von Apps....110
17.5 Konfigurieren von VPN pro App und Einstellungen für iOS-Apps....111
17.6 Deinstallation von Apps....112
18 Verteilen von Unternehmensdokumenten....113
18.1 Hinzufügen von Unternehmensdokumenten....113
19 Verwalten von Geräten....115
19.1 Einsehen von Geräten....115
19.2 Bearbeiten von Geräten....118

19.3 Deregistrieren von Geräten....119
19.4 Gerätegruppen....120
20 Provisionieren von Geräten über die Sophos Mobile Control Web-Konsole....121
20.1 Einrichten einzelner Geräte....121
20.2 Provisionieren einzelner Windows Mobile-Geräte....121
21 Administratoren anlegen....123
22 Senden von Nachrichten an Geräte....124
22.1 Senden von Nachrichten an einzelne Geräte....124
23 Lizenzen für die Verwaltung von Sophos Mobile Security und Sophos Secure Workspace....125
23.1 Aktivierung von Lizenzen für lokale Installationen....125
23.2 Aktivieren von Lizenzen für Software as a Service Installationen....125
24 Verwaltung von Sophos Mobile Security über Sophos Mobile Control....126
24.1 Konfigurieren von Antivirus Einstellungen für Sophos Mobile Security....126
24.2 Konfigurieren von Webfilter-Einstellungen für Sophos Mobile Security....128
24.3 Definieren von Sophos Mobile Security Compliance-Einstellungen....129
24.4 Einsehen von Sophos Mobile Security Scan-Ergebnissen....130
25 Verwaltung von Sophos Secure Workspace über Sophos Mobile Control....132
25.1 Konfigurieren von Sophos Secure Workspace....132
25.2 Zurücksetzen des Kennworts für die Sophos Secure Workspace App....133
25.3 Einrichten des Dokumentenzugriffs - Sophos Secure Workspace sperren und entsperren....133
26 Technischer Support....135
27 Rechtliche Hinweise....136

1 Über Sophos Mobile Control

Sophos Mobile Control ist eine Device Management Lösung für Mobilgeräte wie Smartphones und Tablets. Sophos Mobile Control hilft Ihnen, Ihre Unternehmensdaten durch die Verwaltung und Steuerung von Apps und Sicherheitseinstellungen zu schützen. Sophos Mobile Control ermöglicht Konfiguration, Software-Verteilung, Definition von Sicherheitseinstellungen und viele andere Mobile Device Management Funktionen bei Mobilgeräten.

Das Sophos Mobile Control System besteht aus einer Server- und einer Client-Komponente, die über Datenverbindungen und Textnachrichten kommunizieren.

Der Sophos Mobile Control Client lässt sich schnell und einfach installieren und verwalten. Dies wird durch Over-the-air-Setup und Konfiguration über die Sophos Mobile Control Web-Konsole erreicht.

Mit dem Sophos Mobile Control Self Service Portal für Ihre Benutzer können Sie den Aufwand für die IT verringern, indem Sie die Benutzer dazu berechtigen, ihre eigenen Geräte zu registrieren und andere Aufgaben auszuführen, ohne dass Unterstützung durch das Helpdesk erforderlich ist.

Sophos Mobile Control unterstützt folgende Plattformen für Mobilgeräte:

- Android
- Apple iOS
- Windows Phone 8

Die unterstützten Funktionen können je nach Plattform variieren. Im *Sophos Mobile Control Technical Guide* (Englisch) finden Sie eine Matrix der für die verschiedenen Plattformen unterstützten Features.

1.1 Sophos Mobile Control als lokale Installation und "as a Service"

Sophos Mobile Control wird in zwei Liefermodellen angeboten:

- **Sophos Mobile Control für die lokale Installation**

  Mit einer lokalen Installation behalten Sie alle Ihre Daten im Haus und auf Ihrem Server. Diese Variante ist für eine große Anzahl an Benutzern gedacht und bietet erweiterte Managementfunktionen, zum Beispiel:

  - Steuerung des Zugriffs auf Unternehmens-E-Mails
  - Automatische Zuweisung von Geräten zu vorhandenen Gruppen über Ihr Directory
  - Kundenverwaltung mit dem Superadministrator-Kunden, siehe *Sophos Mobile Control Super Administrator Guide* (Englisch).

- **Sophos Mobile Control as a Service**

  Für unsere Software as a Service Version ist auf Ihrer Seite keine Hardware erforderlich. Sophos Mobile Control wird nicht am Unternehmensstandort installiert. Sophos Mobile Control as a Service ist ideal bei eingeschränkten Ressourcen im IT-Bereich. Für die Installation und den Betrieb von Sophos Mobile Control sind keine Ressourcen erforderlich. Wie bei einer lokalen Installation verwaltet ein Administrator die Geräte über die

Web-Konsole. Mit Sophos Mobile Control as a Service können Sie bei kleineren Benutzergruppen schnell und einfach mit Sophos Mobile Control starten.

Die Unterschiede zwischen lokalen Installationen und Sophos Mobile Control as a Service sind in diesem Handbuch gekennzeichnet.

1.2 Einleitung

Dieses Handbuch beschreibt die Benutzung der Sophos Mobile Control Administrations-Web-Konsole.

Eine Beschreibung der Sophos Mobile Control Installation finden Sie im *Sophos Mobile Control Installation Guide* (Englisch).

Hinweis: Der in diesem Handbuch beschriebene Installationsvorgang ist für Sophos Mobile Control as a Service nicht relevant.

Informationen zur Benutzung der Sophos Mobile Control Web-Konsole als Superadministrator für das Kundenmanagement finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

Hinweis: Der *Sophos Mobile Control Super Administrator Guide* ist für Sophos Mobile Control as a Service nicht relevant. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

Eine Beschreibung der wichtigsten Schritte für die Erstkonfiguration finden Sie in den *Sophos Mobile Control und Sophos Mobile Control as a Service Startup-Anleitungen*.

Informationen zur Benutzung des Sophos Mobile Control Self Service Portal finden Sie in den *Sophos Mobile Control Benutzerhandbüchern*.

1.2.1 Terminologie

In diesem Handbuch werden folgende Begriffe verwendet:

Begriff	Erklärung
Gerät	Das Mobilgerät, das verwaltet werden soll (zum Beispiel Smartphone oder Tablet).
Sophos Mobile Control Client	Die Sophos Mobile Control Client Komponente, die auf dem Gerät installiert ist.
Endbenutzer	Der Endbenutzer des Geräts.
Web-Konsole	Die Web-Oberfläche des Servers, die zur Verwaltung der Geräte benutzt wird.
Kunde	Der Mandant, der Geräte verwaltet.
Bereitstellung	Der Vorgang der Ausstattung von Geräten mit Sophos Mobile Control. **Hinweis:** Dieser Vorgang wird auch als „Enrollment“ oder „Provisioning“ bezeichnet.

Begriff	Erklärung
Auftragspaket	Ein Paket, das Sie zum Bündeln mehrerer Aufträge für Mobilgeräte in einer Transaktion in der Web-Konsole erstellen können. Sie können alle Aufträge bündeln, die zur vollständigen Registrierung eines Geräts notwendig sind.
Self Service Portal (SSP)	Die Sophos Mobile Control Web-Schnittstelle, mit dem Endbenutzer ihre eigenen Geräte registrieren und andere Aufgaben ausführen können. Hierzu ist keine Unterstützung durch den Helpdesk erforderlich.
Sophos Mobile Security	Eine Security App für Android-Mobiltelefone und Tablets, die von Sophos Mobile Control aus verwaltet werden kann. Sophos Mobile Security Management ist ein optionales Modul von Sophos Mobile Control. Zum Verwalten der Sophos Mobile Security App von Sophos Mobile Control aus muss eine SMC Advanced-Lizenz verfügbar sein. Diese Lizenz muss in der Sophos Mobile Control Web-Konsole aktiviert werden.
SMSec	Abkürzung für Sophos Mobile Security, die in der Benutzeroberfläche von Sophos Mobile Control verwendet wird.
Sophos Secure Workspace	Eine Verschlüsselungs-App für iOS und Android Mobiltelefone und Tablets, die von Sophos Mobile Control aus verwaltet werden kann. Die Sophos Secure Workspace Verwaltungsfunktion ist ein optionales Modul von Sophos Mobile Control. Zum Verwalten der App von Sophos Mobile Control aus muss eine SMC Advanced-Lizenz verfügbar sein. Diese Lizenz muss in der Sophos Mobile Control Web-Konsole aktiviert werden.

2 Über die Sophos Mobile Control Web-Konsole

Die Sophos Mobile Control Web-Konsole ist das zentrale Instrument für das Management von Geräten mit Sophos Mobile Control. Sie ist die Web-Schnittstelle für den für das Device Management benutzten Server. Mit der Web-Konsole können Sie eine unternehmensweite Richtlinie für die Benutzung von Mobilgeräten implementieren und sie auf die in Sophos Mobile Control registrierten Geräte anwenden.

Hinweis: Aufgrund der unterschiedlichen Betriebssysteme für Mobilgeräte variieren die jeweils unterstützten Features. Im *Sophos Mobile Control Technical Guide* (Englisch) finden Sie eine Matrix der für die verschiedenen Gerätetypen unterstützten Features.

In der Sophos Mobile Control Web-Konsole können Sie

- Das System konfigurieren, zum Beispiel persönliche oder plattformspezifische Einstellungen
- Geräterichtlinien konfigurieren und Aktionen festlegen, die ausgeführt werden, wenn Geräte nicht mehr den festgelegten Regeln entsprechen (siehe Konfigurieren von Geräterichtlinien (Seite 35)).
- Geräte bei Sophos Mobile Control registrieren (siehe Hinzufügen von Geräten zu Sophos Mobile Control (Seite 40)).
- Geräte provisionieren (siehe Provisionieren von Geräten über die Sophos Mobile Control Web-Konsole (Seite 121)).
- App-Pakete auf registrierten Geräten installieren (siehe Mit Apps arbeiten (Seite 106)).
- Profile und Sicherheitsrichtlinien für Geräte definieren (siehe Mit Profilen arbeiten (Seite 44)).
- Auftragspakete zum Bündeln mehrerer Aufgaben für Mobilgeräte erstellen und sie in einem Arbeitsschritt übertragen (siehe Mit Auftragspaketen arbeiten (Seite 104)).
- Einstellungen für das Self Service Portal festlegen (siehe Konfigurieren der Benutzung des Self Service Portal für Endbenutzer (Seite 22)).
- Administrative Aufgaben auf Geräten durchführen, zum Beispiel das Kennwort für Geräte zurücksetzen, Geräte bei Verlust oder Diebstahl sperren oder zurücksetzen, Geräte deregistrieren (siehe Verwalten von Geräten (Seite 115)).
- Berichte erstellen und einsehen (siehe Dashboard (Seite 14) und Reports (Seite 15)).

2.1 Voraussetzungen

Damit Sie die Sophos Mobile Control Web-Konsole benutzen können, müssen folgende Voraussetzungen erfüllt sein:

- Sie benötigen einen mit dem Internet verbundenen Computer mit einem Internet-Browser. Informationen zu den unterstützten Browsern und den relevanten Versionen finden Sie in den *Sophos Mobile Control Release Notes*.
- In der Web-Konsole muss ein Kunde (ein Mandant, dessen Geräte in Sophos Mobile Control verwaltet werden) vorhanden sein. Kunden werden von Superadministratoren erstellt. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

Hinweis: Für Sophos Mobile Control as a Service wird ein Kunde vordefiniert. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

- Sie benötigen ein Sophos Mobile Control Benutzerkonto und die relevanten Anmeldedaten für die Anmeldung an der Web-Konsole. Die Anmeldedaten bestehen aus Kunde, Benutzer und Kennwort. Für weitere Informationen siehe Erste Anmeldung (Seite 11).

2.2 Web-Konsolen-Benutzer

Die Benutzer der Web-Konsole können unterschiedliche Rollen haben. Sie können diese Rollen zuweisen, wenn Sie neue Administratoren in der Web-Konsole anlegen, siehe Administratoren anlegen (Seite 123).

Die in der Web-Konsole verfügbaren Module/Funktionen richten sich nach der Rolle.

Sie können folgende Rollen zuweisen:

Rolle	Beschreibung
Administrator	Hat die Berechtigung, alle verfügbaren Aktionen auszuführen.
Benutzer	Ist zur Durchführung von Aktionen berechtigt, die für die Installation und Verwaltung eines Mobilgeräts erforderlich sind. Die Berechtigungen umfassen jedoch nicht grundlegende Einstellungen (z. B. Ändern eines Client-Pakets oder einer Vorlage).
Helpdesk	Diese Rolle ist nur für Support-Zwecke gedacht. Sie hat nur eingeschränkte Berechtigungen (z. B. Installation von Softwarepaketen). Diese Rolle hat keinen Zugriff auf kritische Funktionen, zum Beispiel die Definition von Einstellungen und das Erstellen, Löschen oder Bearbeiten von Geräten/Gerätegruppen, Paketen und Profilen.

Wenn Sie weitere Rollen benötigen, wenden Sie sich bitte an den Sophos Support.

3 Wichtige Schritte für das Management von Geräten mit der Web-Konsole

Sophos Mobile Control bietet eine breite Palette von Mobile Device Management Funktionen je nach Gerätetyp, unternehmensweiten Sicherheitsrichtlinien und spezifischen Anforderungen im Unternehmen.

Die wichtigsten Schritte für das Management von Mobilgeräten mit Sophos Mobile Control sind:

- Konfigurieren von Compliance-Einstellungen für Geräte in der Web-Konsole (siehe Konfigurieren von Geräterichtlinien (Seite 35)).
- Informationen zum Anlegen von Gerätegruppen finden Sie unter Erstellen von Gerätegruppen (Seite 40).

  Gerätegruppen dienen zur Kategorisierung von Geräten. Wir empfehlen, Geräte zu gruppieren. Da sich Aufgaben auch bei Gerätegruppen statt bei Einzelgeräten ausführen lassen, können Sie Geräte so effizient verwalten.

- Informationen zum Registrieren und Provisionieren von Geräten finden Sie unter Hinzufügen von Geräten zu Sophos Mobile Control (Seite 40) und Provisionieren von Geräten über die Sophos Mobile Control Web-Konsole (Seite 121).

  Geräte können entweder von Administratoren über die Web-Konsole, oder von Geräteendbenutzern über das Self Service Portal registriert und provisioniert werden. In der Web-Konsole können Sie Einstellungen für das Self Service Portal konfigurieren und Self Service Portal Benutzer verwalten.

- Informationen zum Einrichten von Profilen und Sicherheitseinstellungen für Geräte in der Web-Konsole finden Sie unter Mit Profilen arbeiten (Seite 44).
- Informationen zum Erstellen von Auftragspaketen für die Self Service Portal-Konfiguration finden Sie unter Mit Auftragspaketen arbeiten (Seite 104).
- Informationen zum Konfigurieren der Nutzung des Self Service Portal für Endnutzer finden Sie unter Konfigurieren der Benutzung des Self Service Portal für Endbenutzer (Seite 22).
- Anwenden von neuen oder aktualisierten Profilen und Sicherheitseinstellungen auf registrierte Geräte

4 Anmelden an der Sophos Mobile Control Web-Konsole

4.1 Erste Anmeldung

Voraussetzung: Bevor Sie sich zum ersten Mal bei der Sophos Mobile Control Web-Konsole anmelden, müssen Sie sicherstellen, dass in der Web-Konsole ein Benutzerkonto für Sie erstellt wurde und Sie die Anmeldedaten für dieses Konto (Kunde, Benutzer und Einmalkennwort) besitzen. Das Benutzerkonto kann vom Superadministrator oder von einem anderen Administrator-Benutzer der Web-Konsole angelegt worden sein. Weitere Informationen zum Superadministrator finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Weitere Informationen zum Anlegen neuer Web-Konsolen-Benutzer finden Sie unter Administratoren anlegen (Seite 123).

Hinweis: Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt. Weitere Informationen zur ersten Anmeldung an Sophos Mobile Control as a Service finden Sie in der *Sophos Mobile Control as a Service Startup-Anleitung*.

1. Öffnen Sie die Web-Konsole.

   Der Web-Konsole-Anmeldedialog wird angezeigt.

2. Geben Sie **Kunden**, **Benutzer** Namen und das einmal zu verwendende **Kennwort** ein und klicken Sie auf **Einloggen**.

   Sie werden an der Sophos Mobile Control Web-Konsole angemeldet und dazu aufgefordert, Ihr Kennwort zu ändern.

3. Geben Sie ein neues Kennwort ein, bestätigen Sie es und klicken Sie auf die **Speichern** Schaltfläche.

Eine Meldung bestätigt, dass die Änderungen gespeichert wurden. Sie können nun das neue Kennwort zum Anmelden verwenden.

4.2 Anmeldung

1. Öffnen Sie die Web-Konsole.

   Der Web-Konsole-Anmeldedialog wird angezeigt.

2. Geben Sie **Kunden**, **Benutzer** Namen und **Kennwort** ein und klicken Sie auf **Einloggen**.

Sie werden an der Web-Konsole angemeldet. Die **Startseite** Ansicht des Kunden, an dem Sie sich angemeldet haben, wird angezeigt.

4.3 Ändern Ihres Kennworts

Sie können nach der Anmeldung an der Web-Konsole Ihr Kennwort jederzeit ändern.

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Setup** und dann auf **Allgemein** und gehen Sie zur Registerkarte **Kennwort ändern**.

2. Geben Sie das alte Kennwort sowie ein neues Kennwort ein und bestätigen Sie das neue Kennwort.
3. Klicken Sie auf die **Speichern** Schaltfläche.

4.4 Kennwort-Recovery

Wenn Sie Ihr Kennwort für die Anmeldung an der Web-Konsole vergessen haben, können Sie es zurücksetzen, um ein neues Kennwort zu erhalten.

1. Klicken Sie im **Anmeldedialog** der Web-Konsole auf **Kennwort vergessen?**.

   Der **Kennwort zurücksetzen** Dialog wird angezeigt.

2. Geben Sie Ihre Informationen in die Felder **Kunde** und **Benutzer** ein und klicken Sie auf **Kennwort zurücksetzen**.

   Sie erhalten eine E-Mail mit einem Link zum Zurücksetzen Ihres Kennworts.

3. Klicken Sie auf den Link.

   Der Dialog **Kennwort ändern** wird angezeigt.

4. Geben Sie ein neues Kennwort ein, bestätigen Sie es und klicken Sie auf **Kennwort ändern**.

Ihr Kennwort wurde geändert und Sie sind bei der Web-Konsole angemeldet.

4.5 Abmelden

Um sich von der Web-Konsole abzumelden, klicken Sie im Header auf **Abmelden**.

5 Die Benutzeroberfläche der Web-Konsole

Die Benutzeroberfläche von Sophos Mobile Control unterteilt sich in Header, Hauptmenü und Hauptfenster. In Letzterem wird der Inhalt des aktuell aktiven Menüs angezeigt.

- **Header**

  Im Header finden Sie:

  - Den Benutzernamen des aktuell eingeloggten Benutzers und den Kunden
  - Die Schaltfläche **Hilfe** zum Aufrufen der Online-Hilfe
  - Die Schaltfläche **Abmelden** zum Abmelden des aktuell eingeloggten Benutzers

- **Hauptmenü**

  Über das Hauptmenü auf der linken Seite haben Sie Zugriff auf alle Funktionen von Sophos Mobile Control.

Hinweis: Welche Funktionen in der Web-Konsole verfügbar sind, hängt von der Rolle des eingeloggten Benutzers ab. Siehe Web-Konsolen-Benutzer (Seite 9). Für Superadministratoren zeigt die Web-Konsole eine spezifische Ansicht für den Superadministrator-Kunden. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

6 Dashboard

Das individualisierbare **Dashboard** ist die reguläre Startseite von Sophos Mobile Control und bietet die wichtigsten Informationen auf einen Blick. Es enthält mehrere Widgets, die Informationen liefern über:

- Geräte (alle oder nach Gruppe)
- Compliance-Status Ihrer Geräte, sortiert nach Plattform
- Managed-Status nach Plattform oder für alle Geräte
- SSP-Registrierungsstatus
- Plattformversionen, die in Verwendung sind

Klicken Sie auf **Widget hinzufügen**, um die angezeigten Informationen an Ihre Erfordernisse anzupassen.

Klicken Sie auf **Standardlayout wiederherstellen**, um die Sophos Mobile Control **Dashboard**-Standardansicht wiederherzustellen.

Hinweis: Im Superadministrator-**Dashboard** sind alle Kunden aufgelistet.

7 Reports

In der Web-Konsole unter **Reports** stehen die folgenden Reports für Superadministratoren und Administratoren zur Verfügung:

- Geräte-Reports
  - Geräte
  - Geräte pro Benutzer
  - Anzahl von Geräten pro Betriebssystem
  - Geräte, die in den letzten 7 Tagen eingerichtet wurden
  - Geräte, die sich in den letzten 7 Tagen nicht synchronisiert haben
  - Geräte, die sich in den letzten 7 Tagen abgemeldet haben
  - Geräte, die in den letzten 7 Tagen zurückgesetzt wurden
- App-Reports
  - Apps auf allen Plattformen
  - Anzahl der Apps auf allen Plattformen
  - Apps auf Android
  - Apps auf iOS
- Compliance-Reports
  - Richtlinienverletzungen
  - Anzahl der Richtlinienverletzungen

Klicken Sie auf einen Report, um die Informationen in eine Microsoft Excel-Datei zu exportieren.

8 Aufträge

Die Auftragsansicht vermittelt einen Überblick über alle Aufträge, die Sie erstellt und begonnen haben, mit Angabe des aktuellen Status.

Sie können die Aufträge nach **Typ** und **Status** filtern.

Sie können alle Ihre Aufträge überwachen und bei Problemen eingreifen. Sie können beispielsweise einen Auftrag löschen, der offensichtlich nicht abgeschlossen werden kann, aber das Gerät blockiert.

Um einen Auftrag zu löschen, wählen Sie diesen aus und klicken Sie auf **Löschen** (Papierkorb-Symbol).

Sie können die Einträge nach **Typ** und **Status** filtern und nach Name des **Geräts**, Name des **Pakets**, Erstelldatum und Auftragsdatum sortieren.

8.1 Überwachen von Aufträgen in der Web-Konsole

Sie können alle vorhandenen Aufträge für Geräte in der Web-Konsole überwachen:

- Die Ansicht **Aufträge** zeigt alle noch nicht abgeschlossenen und fehlgeschlagenen Aufträge sowie die abgeschlossenen Aufträge der letzten Tage an. Die **Auftragsstatus** Ansicht wird automatisch aktualisiert. Sie können somit den Fortschritt der Aufträge verfolgen.
- Die Ansicht **Auftragsdetails** zeigt allgemeine Informationen zu einem Auftrag aus der Ansicht **Aufträge** oder dem **Auftragsarchiv** an.
- Das **Auftragsarchiv** zeigt alle Aufträge.

8.1.1 Einsehen von nicht abgeschlossenen, fehlgeschlagenen und zuletzt abgeschlossenen Aufträgen

1. Die Spalte **Status** in der **Auftragsansicht** zeigt den Auftragsstatus an, zum Beispiel **Endgültig fehlgeschlagen**.
2. Im Feld **Aktualisierungsintervall (in Sek.)** können Sie auswählen, wie oft der **Auftragsstatus** aktualisiert werden soll.
3. Um weitere Details zu einem Auftrag einzusehen, klicken Sie auf das **Anzeigen** Lupensymbol neben den gewünschten Auftrag.

   Die **Auftragsdetails** Ansicht wird angezeigt. Neben allgemeinen Informationen zum Auftrag (z. B. **Gerät**, **Paketname** und **Erstellt am**) werden Angaben zu den Status, die ein bestimmter Auftrag durchlaufen hat, mit Zeitstempeln und Fehlercodes angezeigt. Wenn Kommandos vom Gerät auszuführen sind, wird in der **Auftragsdetails** zusätzlich eine **Details** Schaltfläche angezeigt.

4. Klicken Sie auf die **Details** Schaltfläche, falls verfügbar, um das vom Gerät auszuführende Kommando einzusehen.

   Die Ansicht **Kommandos** mit den relevanten Kommandos wird angezeigt. Die an das Gerät geschickten Kommandos sind Teil des Auftrags. Sie werden vom Client ausgeführt. Die Ergebnisse, die Erfolg oder Fehlschlag angeben, werden an den Server zurück gesendet. Ist kein Fehler aufgetreten, so lautet der Fehlercode "0". Ist ein Kommando fehlgeschlagen, so wird der entsprechende Fehlercode angezeigt. Meistens werden auch Informationen dazu angezeigt, was den Fehlschlag verursacht haben könnte.

5. Um in die **Auftragsdetails** Ansicht zurückzukehren, klicken Sie auf die **Zurück** Schaltfläche.
6. Um fehlgeschlagene Aufträge manuell erneut auszuführen, klicken Sie auf die **Jetzt ausführen** Schaltfläche.

   Hinweis: Diese Schaltfläche wird nur für fehlgeschlagene Aufträge angezeigt. Sie können nur Aufträge erneut ausführen, die noch nicht vollständig fehlgeschlagen sind.

8.1.2 Einsehen des Auftragsarchivs

1. Klicken Sie in der Ansicht **Auftrag** auf die Schaltfläche **Auftragsarchiv**.

   Die **Auftragsarchiv** Ansicht wird angezeigt. Sie zeigt alle abgeschlossenen und fehlgeschlagenen Aufträge im System.

2. In dieser Ansicht haben Sie folgende Möglichkeiten:
   - Klicken Sie auf die **Neu laden** Schaltfläche, um die **Auftragsarchiv** Ansicht zu aktualisieren.
   - Wählen Sie Aufträge aus und klicken Sie auf **Löschen** (Papierkorb-Symbol), um sie aus dem Archiv zu löschen.

8.1.3 Auftragsstatus

Die folgende Tabelle enthält einen Überblick zu den in der **Auftragsansicht** und im **Auftragsarchiv** angezeigten Auftragsstatus.

Farbsymbol	Status	Beschreibung
	Angenommen	Der Auftrag wurde erstellt.
	Wiederholung	Der Auftrag wird später wiederholt.
	Gestartet	Der Auftrag wurde gestartet.
	In Bearbeitung	Die Ausführung des Auftrags wird vorbereitet.
	Sende Benachrichtigung	Der Client wird benachrichtigt
	Warte auf Zustellung	Der Server wartet auf die Bestätigung der Benachrichtigung durch den Client.

Farbsymbol	Status	Beschreibung
🟡	Benachrichtigung	Der Client hat die Benachrichtigung erhalten.
🟡	Ausgeliefert	Der Client hat das Paket bzw. die Kommandos erhalten.
🟡	Ergebnisauswertung gestartet.	Der Client hat geantwortet und die Auswertung des Ergebnisses wurde gestartet.
🟡	Ergebnis unvollständig	Die Ergebnisauswertung hat gezeigt, dass nicht alle Ergebnisse des Kommandos eingegangen sind.
🟢	Erfolgreich	Das Paket wurde installiert oder die Kommandos wurden erfolgreich ausgeführt. **Hinweis:** Für die Ersteinrichtung (Provisionierung) des Sophos Mobile Control Client muss der Auftrag mit dem Status "Installiert " abgeschlossen werden.
🟢	Installiert	Der Sophos Mobile Control Client wurde erfolgreich installiert. Das Gerät ist nun provisioniert.
🔴	Ergebnisauswertung fehlgeschlagen	Die Ergebnisauswertung konnte nicht durchgeführt werden.
🔴	Auftrag teilweise fehlgeschlagen	Nicht alle Kommandos des Auftrags konnten erfolgreich ausgeführt werden.
🔴	Verschoben	Der Auftrag wird später neu gestartet.
🔴	Fehlgeschlagen (wird wiederholt)	Der Auftrag ist fehlgeschlagen und wird später wiederholt.
🔴	Auftrag fehlgeschlagen	Der Auftrag ist fehlgeschlagen und wird nicht wiederholt.
🔴	Endgültig fehlgeschlagen	Der Auftrag ist fehlgeschlagen.

9 Allgemeine Einstellungen

In der Ansicht **Allgemeine Einstellungen** können Sie die Grundeinstellungen für Sophos Mobile Control vornehmen.

9.1 Persönliche Einstellungen

Damit Sie die Sophos Mobile Control Web-Konsole möglichst effizient nutzen können, lässt sich die Benutzeroberfläche so anpassen, dass nur die Plattformen, mit denen Sie arbeiten möchten, angezeigt werden.

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Einstellungen** und dann auf **Allgemein**.

   Die **Allgemeine Einstellungen** Ansicht wird angezeigt.

2. Wechseln Sie zur Registerkarte **Persönlich**.
3. Konfigurieren Sie folgende Einstellungen:

   a) Wählen Sie im Feld **Sprache** die Sprache für die Sophos Mobile Control Web-Konsole aus.

   b) Wählen Sie im Feld **Zeitzone** die gewünschte Zeitzone aus.

   c) Wählen Sie im Feld **Datensätze pro Tabellenseite** die maximale Anzahl an Tabellenzeilen aus, die in der Web-Konsole pro Seite angezeigt werden sollen. Sie können zwischen **20** und **100** Zeilen auswählen.

   d) Wählen Sie **Erweiterte Gerätedetails anzeigen**, um alle verfügbaren Informationen zu dem Gerät anzuzeigen. Die Registerkarten **Eigene Eigenschaften** und **Interne Eigenschaften** werden der Ansicht **Gerät anzeigen** hinzugefügt.

   e) Wählen Sie unter **Aktivierte Plattformen** die Plattformen aus, die Sie in der Web-Konsole benutzen möchten: **Android**, **iOS** und **Windows Phone** werden unterstützt. Wenn Sie spezifische Plattformen auswählen, können Sie nur diese Plattformen mit Sophos Mobile Control verwenden. Alle anderen Plattformen werden verborgen. Darüber hinaus werden alle Module und Funktionen verborgen, die für eine spezifische Plattform nicht benötigt werden.

   Hinweis: Die Liste der verfügbaren Plattformen richtet sich nach den Einstellungen aus der Super-Administrator-Konfiguration. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

   Das Menü wird entsprechend Ihren Einstellungen angepasst. Funktionen, die nicht benötigt werden, werden ausgeblendet.

4. Klicken Sie auf die **Speichern** Schaltfläche.

9.2 Kennwortrichtlinien

Konfigurieren Sie zur Durchsetzung der Sicherheit von Kennwörtern Kennwortrichtlinien für Benutzer der Sophos Mobile Control Web-Konsole und des Self Service Portal.

Hinweis: Wenn Sie interne Benutzerverwaltung anwenden, gelten die Kennwortrichtlinien für die Web-Konsolen-Benutzer und die Self Service Portal Benutzer. Wenn Sie die externe Benutzerverwaltung nutzen, gelten die Kennwortrichtlinien nur für die Web-Konsolen-Benutzer.

In dieser Anleitung wird als Beispiel die interne Self Service Portal Benutzerverwaltung beschrieben. Weitere Informationen zur externen Benutzerverwaltung finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Einstellungen** und dann auf **Allgemein**.

   Die **Allgemeine Einstellungen** Ansicht wird angezeigt.

2. Wechseln Sie zur Registerkarte **Kennwortrichtlinien**.
3. Definieren Sie unter **Kennwortrichtlinien für SMC Web-Konsolen-Benutzer** - **Regeln** die erforderlichen Mindestwerte für das Kennwort.
4. Legen Sie unter **Kennwortrichtlinien für SMC Web-Konsolen-Benutzer** - **Einstellungen** die folgenden Einstellungen fest:
   - **Änderungsintervall (Tage)**: Sie können einen Wert zwischen **0** (keine Kennwortänderung erforderlich) und **730** Tagen eingeben.
   - **Anzahl der letzten Kennwörter, die nicht benutzt werden dürfen**: Sie können einen Wert zwischen **1** und **10** auswählen.
   - **Maximale Anzahl fehlerhafter Loginversuche**: Sie können einen Wert zwischen **1** und **10** auswählen.
5. Klicken Sie auf die **Speichern** Schaltfläche.

9.3 iOS-Client

Mit Sophos Mobile Control können Sie die Position Ihrer Geräte bestimmen und deren Standort jederzeit anzeigen. Geräte früherer Versionen haben ihren Standort in festgelegten Intervallen gemeldet.

Sie können Sophos Mobile Control so konfigurieren, dass diese alte Positionsbestimmungsmethode verwendet wird.

Aktivieren Sie dazu die Option **Verwendung der alten Positionsbestimmungsmethode erzwingen**.

Hinweis: Wenn Sie diese Funktion aktivieren, verringert sich die Akkulaufzeit.

9.4 Windows Phone-Client

Für Windows Phone 8.0-Geräte können Sie das MDM-Polling-Intervall konfigurieren. Wählen Sie das Intervall aus der Dropdown-Liste aus.

Hinweis: Die Synchronisierung wird nur in diesem Intervall durchgeführt. Die Synchronisierung lässt sich nicht über den Server auslösen. Das Poll-Intervall betrifft nur Windows Phone 8.0-Geräte. Neuere Geräte können Push-Benachrichtigungen empfangen und pollen darüber hinaus standardmäßig alle 24 Stunden.

Mit dieser Version von Sophos Mobile Control können Sie Ihre Geräte lokalisieren und deren Standort jederzeit anzeigen. Geräte früherer Versionen haben ihren Standort in festgelegten Intervallen gemeldet.

Wenn Sie die Option **Alte Positionsbestimmungsmethode aktivieren** aktivieren, bestimmt die auf Windows Phone 8-Geräten installierte Sophos Mobile Control App die Position des Geräts und sendet diese an den Sophos Mobile Control Server.

Wählen Sie im Feld **Gewünschte Genauigkeit (in Metern)** den Radius für durch die Funktion **Position anzeigen** erfasste Positionsänderungen aus.

Hinweis: Wenn Sie diese Funktion aktivieren, verringert sich die Akkulaufzeit. Benötigt wird sie nur für Windows Phone 8.0-Geräte. Bei neueren Geräten erfolgt die Positionsbestimmung nur auf Anfrage.

9.5 E-Mail-Konfiguration

Auf der Registerkarte **E-Mail-Konfiguration** können Sie Einstellungen für E-Mails festlegen, die an Benutzer gesendet werden.

Wählen Sie die Sprache für die E-Mails aus der Dropdown-Liste neben der Option **Standardsprache** aus und geben Sie die Absender-E-Mail-Adresse in das Textfeld ein.

9.6 Technischer Kontakt

Um Benutzer bei Fragen oder Problemen zu unterstützen, können Sie Informationen zu einem technischen Kontakt konfigurieren. Die Informationen, die Sie hier eingeben, werden in der Sophos Mobile Control App und im Self Service Portal angezeigt.

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Einstellungen** und dann auf **Allgemein**.

   Die **Allgemeine Einstellungen** Ansicht wird angezeigt.

2. Wechseln Sie in die Registerkarte **Technischer Kontakt**.
3. Geben Sie die erforderlichen Informationen für den technischen Kontakt ein. Unter **Zusatzinformation** können Sie Informationen für den Support von Benutzern bei Fragen oder Problemen eingeben.
4. Klicken Sie auf die **Speichern** Schaltfläche.

10 Konfigurieren der Benutzung des Self Service Portal für Endbenutzer

Mit dem Self Service Portal können Sie IT-Aufwände reduzieren, indem Sie die Endbenutzer dazu berechtigen, ihre eigenen Geräte zu registrieren und andere Aufgaben auszuführen. Hierzu ist keine Unterstützung durch den Helpdesk erforderlich. Die Benutzung des Self Service Portal wird für folgende Plattformen unterstützt:

- Android
- Apple iOS
- Windows Phone 8

Weitere Informationen zur Benutzung des Self Service Portal finden Sie im *Sophos Mobile Control Benutzerhandbuch.*

In der Web-Konsole können Sie Einstellungen für die Benutzung des Self Service Portal konfigurieren, zum Beispiel für welche Plattformen die Registrierung über das Self Service Portal aktiv sein soll oder welche Funktionen im Self Service Portal zur Verfügung stehen sollen. Sie können außerdem die Benutzer des Self Service Portal verwalten.

10.1 Erstellen von Self Service Portal Gruppen mit der internen Benutzerverwaltung

Self Service Portal Konfigurationen werden auf Gruppen von Self Service Portal Benutzern angewendet. Mit der internen Benutzerverwaltung können Sie Self Service Portal Gruppen erstellen und ihnen Benutzer zuweisen. Für weitere Informationen zur Benutzerverwaltung siehe Verwalten von Self Service Portal Benutzern (Seite 26).

Hinweis: Die interne Benutzerverwaltung steht nur dann für einen Kunden zur Verfügung, wenn sie vom Superadministrator aktiviert wurde. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service gilt. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt. Informationen darüber, wie Sie die Methoden für die Benutzerverwaltung für Sophos Mobile Control as a Service festlegen, finden Sie unter Konfigurieren der Self Service Portal Benutzerverwaltung für Sophos Mobile Control as a Service (Seite 26).

So erstellen Sie eine Self Service Portal Gruppe:

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Benutzer**.

   Die **Benutzer anzeigen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Benutzergruppen anzeigen**.

   Die Ansicht **Benutzergruppen anzeigen** wird angezeigt.

3. Klicken Sie auf die Schaltfläche **Gruppe anlegen**.

   Die **Gruppe bearbeiten** Ansicht wird angezeigt.

4. Geben Sie im Feld **Name** einen Namen für die neue Self Service Portal Gruppe ein.
5. Klicken Sie auf die **Speichern** Schaltfläche.

Die neue Self Service Portal-Benutzergruppe wird in der Ansicht **Benutzergruppen anzeigen** angezeigt. Wenn Sie neue Benutzer erstellen, können Sie diese der Gruppe zuweisen. Wenn Sie Self Service Portal Einstellungen definieren, können Sie die Gruppe auswählen und Ihr die Einstellungen zuweisen.

10.2 Konfigurieren von Self Service Portal Einstellungen

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Setup** und danach auf **Self Service Portal**.

   Die **Self Service Portal** Ansicht wird angezeigt.

2. Konfigurieren Sie in der **Konfiguration** Registerkarte folgende Einstellungen:

   a) Wählen Sie im **Maximale Anzahl an Geräten** Feld die maximale Anzahl an Geräten, die ein Benutzer über das Self Service Portal registrieren kann. Indem Sie hier eine maximale Anzahl festlegen können Sie eine Überschreitung der verfügbaren Lizenzen vermeiden.

   b) Wählen Sie unter **Verfügbare Funktionen** die Funktionen, die Benutzern im Self Service Portal zur Verfügung stehen sollen. Die Funktionen variieren je nach Mobilgerätetyp (Plattform). Im *Sophos Mobile Control Technical Guide* (Englisch) finden Sie eine Matrix der für die verschiedenen Gerätetypen unterstützten Features. Sie können folgende Funktionen auswählen:

   - **Gerät lokalisieren**

     Mit dieser Funktion können Benutzer Ihre Android-, iOS- oder Windows Phone 8-Geräte bei Verlust oder Diebstahl orten.

   - **Gerät sperren**

     Mit dieser Funktion können Benutzer Ihre Geräte bei Verlust oder Diebstahl sperren.

   - **Neukonfiguration**

     Mit dieser Funktion können Benutzer ihre Geräte neu konfigurieren, wenn Sophos Mobile Control vom Gerät entfernt wurde, das Gerät jedoch noch registriert ist.

   - **Richtlinienverletzungen anzeigen**

     Mit dieser Funktion können Benutzer die Compliance-Verletzungen für die für sie registrierten Geräte im Self Service Portal einsehen.

   - **Daten aktualisieren**

     Mit dieser Funktion können Benutzer Ihre Geräte manuell mit dem Sophos Mobile Control Server synchronisieren. Dies ist zum Beispiel nützlich, wenn das Gerät längere Zeit ausgeschaltet war und daher nicht mit dem Server synchronisiert wurde. In diesem Fall ist das Gerät unter Umständen nicht compliant (je nach konfigurierten Compliance-Einstellungen) und muss mit dem Server synchronisiert werden, damit es die Richtlinien wieder erfüllt.

   - **Kennwort zurücksetzen**

     Mit dieser Funktion können Benutzer das Kennwort für das Entsperren des Bildschirms zurücksetzen. Für Android-Geräte wird ein neues Kennwort gesetzt. Das Gerät lässt sich nur mit dem neuen Kennwort entsperren. Für iOS-Geräte wird das Kennwort vollstdändig gelöscht. Der Benutzer muss innerhalb von 60 Minuten ein neues Kennwort definieren.

- **Gerät zurücksetzen**

  Mit dieser Funktion können Benutzer Ihre registrierten Geräte bei Verlust oder Diebstahl auf den Werkszustand zurücksetzen. Alle Daten auf dem Gerät werden gelöscht.

- **Gerät deregistrieren**

  Mit dieser Funktion können Benutzer Geräte deregistrieren, die nicht mehr benutzt werden. Dies ist zum Beispiel nützlich, wenn die Anzahl an Geräten, die Benutzer über das Self Service Portal registrieren können, begrenzt ist.

- **Nicht registriertes Gerät löschen**

  Mit dieser Funktion können Benutzer deregistrierte Geräte löschen. Dies ist zum Beispiel für das Freigeben benutzter Lizenzen nützlich.

- **Zurücksetzen von Kennwörtern für App Protection**

  Mit dieser Funktion können Benutzer ihr App Protection-Kennwort auf Android Geräten zurücksetzen. Das App Kennwort schützt definierte Apps und muss jedes Mal eingegeben werden, wenn Benutzer diese Apps starten. Das Kennwort wird gelöscht und die Benutzer müssen ein neues Kennwort definieren.

- **Kennwort für die Sophos Secure Workspace App zurücksetzen**

  Mit dieser Funktion können Benutzer ihr Kennwort für die Sophos Secure Workspace App zurücksetzen. Das Kennwort für die Sophos Secure Workspace App muss jedes Mal eingegeben werden, wenn Benutzer die App starten. Das Kennwort wird gelöscht und die Benutzer müssen ein neues Kennwort definieren.

- **SMC App neu konfigurieren**

  Mit dieser Funktion können Benutzer eine bereits installierte Sophos Mobile Control App neu konfigurieren.

3. Wechseln Sie in die **Vereinbarungstext** Registerkarte und konfigurieren Sie folgende Einstellungen:

   a) eine Mobil-Richtlinie, einen Disclaimer oder eine Vereinbarung. Dieser Text wird im ersten Schritt angezeigt, wenn Endbenutzer Geräte registrieren. Die Benutzer müssen bestätigen, dass sie diesen Text gelesen haben, um fortfahren zu können.

   Für den Text werden einfache HTML-Formatierungs-Tags unterstützt. Der Text wird entsprechend im jeweiligen Browser angezeigt.

4. Gehen Sie zur Registerkarte **Text nach Installation** und konfigurieren Sie folgende Einstellungen:

   a) einen Text, der im Self Service Portal nach den automatischen Installationsschritten angezeigt wird, um dem Benutzer Hilfestellung bei den darauffolgenden erforderlichen Schritten (z. B. Konfiguration des Servers in der iOS App oder Konfiguration des Android Mail Client) zu geben.

   Für den Text werden einfache HTML-Formatierungs-Tags unterstützt. Der Text wird entsprechend im jeweiligen Browser angezeigt.

5. Wechseln Sie in die Registerkarte **Gruppeeninstellungen**. Auf dieser Registerkarte konfigurieren Sie die Gruppeneinstellungen, zum Beispiel die Gerätegruppen, zu denen über das Self Service Portal registrierte Geräte hinzugefügt werden, und das Auftragspaket, das auf Geräten ausgeführt wird.

Wenn Sie externe Benutzerverwaltung verwenden, können Sie Geräte basierend auf der Zugehörigkeit zu einem externen Benutzerverzeichnis zu Gruppen und Profilen zuweisen.

Hinweis: Die externe Benutzerverwaltung muss für den relevanten Kunden in der Kundenveraltung konfiguriert werden. Informationen zur Konfiguration der externen Benutzerverwaltung für einen Kunden finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service gilt. Informationen darüber, wie Sie die Methoden für die Benutzerverwaltung für Sophos Mobile Control as a Service festlegen, finden Sie unter Konfigurieren der Self Service Portal Benutzerverwaltung für Sophos Mobile Control as a Service (Seite 26).

a) Klicken Sie unter **Gruppeneinstellungen** auf die **Hinzufügen** Schaltfläche.

   Die **Gruppeneinstellungen bearbeiten** Ansicht wird angezeigt.

b) Geben Sie einen **Namen** für die Self Service Portal Konfigurationsgruppe ein.

c) Geben Sie im Feld **Verzeichnisgruppe** die Self Service Portal Gruppe ein, die Sie in der internen oder externen Benutzerverwaltung definiert haben, oder die Active Directory Gruppe mit ihrem vollen LDAP-Pfad oder Platzhaltern. In diesem Feld können Sie mit einem Asterisk (*) als erstes, letztes oder einziges Zeichen mehrere Gruppen angeben. Zum Beispiel: Geben Sie Dev* ein, um alle Gruppennamen, die mit "Dev" beginnen, anzugeben. Geben Sie * ein, um alle verfügbaren Gruppen anzugeben.

d) Legen Sie fest, ob **Vereinbarung** und **Text nach Installation** angezeigt werden sollen.

e) Wählen Sie unter **Einrichtungspaket**, die auszuführenden Auftragspakete.

   Hinweis: Sie müssen die Auftragspakete zuerst in der Web-Konsole anlegen. Wenn Sie noch kein Auftragspaket erstellt haben, aktualisieren Sie die Self Service Portal Einstellungen danach. Weitere Informationen zum Anlegen eines Auftragspakets finden Sie unter Mit Auftragspaketen arbeiten (Seite 104). Für weitere Informationen zu den Anforderungen für ein Auftragspaket, das für die Ersteinrichtung über das Self Service Portal verwendet werden soll, siehe die *Sophos Mobile Control Startup-Anleitung* oder die *Sophos Mobile Control as a Service Startup-Anleitung*.

   Hinweis: Wählen Sie bei Windows Phone 8 ein **Profil** unter **Einrichtungspaket** aus. Bei Windows Phone ist zum Einrichten eines Geräts nur ein Profil erforderlich. Das hier ausgewählte Profil enthält gegebenenfalls bereits alle Einstellungen für Ihre Geräte.

f) Wählen Sie unter **Plattform** die Plattformen aus, die im Self Service Portal zur Verfügung stehen sollen.

g) Wählen Sie unter **Einfügen in Geräteruppe** die Gruppe, zu der das Gerät hinzugefügt werden soll.

   Hinweis: In der Web-Konsole steht eine **Default** Gerätegruppe zur Verfügung. Wenn Sie noch keine eigenen Gerätegruppen definiert haben, können Sie Geräte zu dieser Gruppe hinzufügen. Für weitere Informationen siehe Erstellen von Gerätegruppen (Seite 40).

h) Klicken Sie auf die **Übernehmen** Schaltfläche.

6. Die **Self Service Portal** Ansicht wird angezeigt. Klicken Sie auf die **Speichern** Schaltfläche.

Hinweis: Als Superadministrator können Sie auch einen Standard-Kunden festlegen, an dem sich die Endbenutzer im Self Service Portal anmelden. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch). Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service unterstützt wird. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

10.3 Verwalten von Self Service Portal Benutzern

Sophos Mobile Control bietet verschiedene Verfahren für die Verwaltung von Self Service Portal Benutzern:

- Interne Benutzerverwaltung

  Mit der interenen Benutzerverwaltung können Sie Benutzer durch manuelles Hinzufügen in der Web-Konsole oder durch Importieren aus einer .csv-Datei erstellen.

- Externe Benutzerverwaltung

  Mit der externer Benutzerverwaltung können Sie Geräte zu Gruppen und Profilen auf der Grundlage der Directory-Zugehörigkeit zuweisen.

Hinweis: Das verwendete Verfahren ist kundenspezifisch und wird beim Erstellen des Kunden festgelegt. Weitere Informationen zum Definieren des Verfahrens und zur externen Benutzerverwaltung finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service gilt. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt. Für Informationen zur Definition von Benutzerverwaltungsverfahren für Sophos Mobile Control as a Service, siehe Konfigurieren der Self Service Portal Benutzerverwaltung für Sophos Mobile Control as a Service (Seite 26).

10.3.1 Konfigurieren der Self Service Portal Benutzerverwaltung für Sophos Mobile Control as a Service

Hinweis: Dieser Abschnitt bezieht sich nur auf Sophos Mobile Control as a Service. Wenn Sie Sophos Mobile als lokale Installation einsetzen, wird die Benutzerverwaltung für Benutzer des Self Service Portal vom Superadministrator pro Kunde konfiguriert. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Setup** und dann auf **Systemeinstellungen**.

   Die **Systemeinstellungen** Ansicht wird angezeigt.

2. Wechseln Sie in die Registerkarte **Benutzerverzeichnis**. Wählen Sie in dieser Registerkarte unter die Datenquelle für die mit Sophos Mobile Control zu verwaltenden Self Service Portal (SSP) Benutzer aus.

   - **Kein Verzeichnis. SSP und personalisierte Profile sind nicht verfügbar.**
   - Wählen Sie **Internes Verzeichnis**, um die interne Benutzerverwaltung für Benutzer des Sophos Mobile Control Self Service Portal zu verwenden.
   - Wählen Sie **Externes Verzeichnis**, um externe Benutzerverwaltung für Benutzer des Sophos Mobile Control Self Service Portal zu verwenden.

     Klicken Sie auf **Externes Benutzerverzeichnis konfigurieren**, um Serverdaten festzulegen (siehe Konfigurieren einer externen Verzeichnisverbindung für Active Directory für Sophos Mobile Control as a Service (Seite 27)).

3. Klicken Sie auf die **Speichern** Schaltfläche.

   Wenn Sie **Internes Verzeichnis** oder **Externes Verzeichnis** ausgewählt haben, wird die ausgewählte Option und die Option **Kein Verzeichnis. SSP und personalisierte Profile sind nicht verfügbar** auf der Registerkarte **Benutzerverzeichnis** angezeigt. Wenn Sie Ihre Auswahl nachträglich ändern möchten, wählen Sie zuerst **Kein Verzeichnis. SSP und personalisierte Profile sind nicht verfügbar**, damit wieder alle Optionen zur Verfügung stehen.

   Hinweis: Die Benutzerverwaltungskonfiguration kann nicht geändert werden, solange Geräte mit dem Verzeichnis verbunden sind. Wenn Sie versuchen, die Konfiguration zu ändern, während noch Geräte verbunden sind, wird eine Fehlermeldung angezeigt.

10.3.1.1 Konfigurieren einer externen Verzeichnisverbindung für Active Directory für Sophos Mobile Control as a Service

Hinweis: Dieser Abschnitt bezieht sich nur auf Sophos Mobile Control as a Service. Wenn Sie Sophos Mobile als lokale Installation einsetzen, wird die Benutzerverwaltung für Benutzer des Self Service Portal vom Superadministrator pro Kunde konfiguriert. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Setup** und dann auf **Systemeinstellungen**. Gehen Sie dann zur Registerkarte **Benutzerverzeichnis**.
2. Wählen Sie auf der Registerkarte **Benutzerverzeichnis** die Option **Externes LDAP-Verzeichnis**, um eine externe Benutzerverwaltung für Benutzer des Sophos Mobile Control Self Service Portal zu verwenden.
3. Klicken Sie auf **Externes LDAP konfigurieren**, um die Serverdaten anzugeben.

   Die Ansicht **Serverdetails** wird angezeigt.

4. Geben Sie in dieser Ansicht folgende Informationen ein:

   a) Wählen Sie den **LDAP-Typ** aus. Sophos Mobile Control unterstützt:

   - **Active Directory**
   - **Domino**
   - **eDirectory**
   - **Zimbra**

   b) Geben Sie im Feld **Primäre URL** die URL des Verzeichnisservers ein. Sie können die Server-IP-Adresse oder den Servernamen eingeben. Wählen Sie **SSL**, um **SSL** für die Serververbindung zu verwenden.

   c) Geben Sie im **Backup URL** Feld die URL des Backup-Servers ein. Sie können die Server-IP-Adresse oder den Servernamen eingeben. Wählen Sie **SSL**, um **SSL** für die Serververbindung zu verwenden.

   d) Geben Sie im Feld **Benutzer** einen Benutzer ein, der Leserechte für den Verzeichnisserver hat. Sie müssen den Benutzer mit der relevanten Domäne eingeben. Folgende Formate werden unterstützt: <Domäne>\<Benutzername> oder <Benutzername>@<Domäne>.<Domänencode>.

   e) Geben Sie im Feld **Kennwort** das Kennwort für den Benutzer ein.

   Klicken Sie auf **Next**.

   Die Ansicht **Suchbasis** wird angezeigt.

5. Wählen Sie die Suchbasis des externen Verzeichnisses aus. Die Suchbasis legt fest, wo nach dem Benutzer/der Gruppe gesucht werden soll, der/die versucht, sich am Self Service Portal anzumelden. Klicken Sie auf **Next**.

   Die Ansicht **Suchfelder** wird angezeigt.

6. In diesem Schritt legen Sie fest, welche Verzeichnisfelder zum Auflösen der Platzhalter %_USERNAME_% und %_EMAILADRESS_% in Profilen verwendet werden. Wählen Sie die erforderlichen Felder aus den Dropdown-Listen **Benutzername** und **E-Mail** aus.
7. Klicken Sie auf **Next**.

   Die Ansicht **SSP Konfiguration** wird angezeigt.

8. Geben Sie im **SSP Gruppe** Feld den Namen der Gruppe ein, die sich am Self Service Portal anmelden darf. Diese Gruppe muss auf dem Verzeichnisserver definiert sein. Alle Mitglieder dieser Gruppe können auf das Self Service Portal zugreifen. Wenn Sie den Zugriff nicht auf eine einzelne Gruppe beschränken möchten, geben Sie * ein, damit alle authentifizierten Verzeichnisbenutzer Zugriff auf das Self Service Portal haben. Wenn Sie die Gruppe eingegeben haben, klicken Sie auf die Schaltfläche **Gruppe finden**, um den Gruppennamen in einen vollständigen Distinguished Name (DN) aufzulösen.
9. Klicken Sie **Übernehmen**.
10. Klicken Sie auf die **Fertigstellen** Schaltfläche.

    Die **Systemeinstellungen** Ansicht wird wieder angezeigt.

11. Klicken Sie auf die **Speichern** Schaltfläche, um Ihre Änderungen zu speichern.

10.3.2 Erstellen von Self Service Portal Benutzern mit der internen Benutzerverwaltung

Voraussetzung: Die interne Benutzerverwaltung ist für den Kunden, an dem Sie angemeldet sind, aktiviert. Für lokale Installationen erfolgt dies durch den Superadministrator in der Kundenverwaltung. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service gilt. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt. Informationen darüber, wie Sie die Methoden für die Benutzerverwaltung für Sophos Mobile Control as a Service festlegen, finden Sie unter Konfigurieren der Self Service Portal Benutzerverwaltung für Sophos Mobile Control as a Service (Seite 26).

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Benutzer**.

   Die **Benutzer anzeigen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Benutzer anlegen**.

   Die **Benutzer bearbeiten** Ansicht wird angezeigt.

3. Definieren Sie in der **Benutzer bearbeiten** Ansicht die folgenden Einstellungen:

   a) **Benutzername**

   b) **Vorname**

   c) **Nachname**

   d) **E-Mail-Adresse**

   e) **Gruppen** (optional)

Klicken Sie auf **Anzeigen**, um alle verfügbaren Benutzergruppen anzuzeigen, und wählen Sie eine Gruppe aus.

4. Klicken Sie auf die **Speichern** Schaltfläche.

Der neue Self Service Portal Benutzer wird in der **Benutzer anzeigen** Ansicht angezeigt. Eine Willkommen-E-Mail wird an den neuen Benutzer gesendet.

Wenn Sie auf das blaue Dreieck neben dem betreffenden Benutzer klicken, können Sie die Benutzerinformationen anzeigen (**Anzeigen**) oder den Benutzer **Bearbeiten** oder **Löschen**.

Hinweis: Wenn Sie auf einen Benutzernamen klicken, wird die Ansicht **Benutzer anzeigen** angezeigt. Diese Ansicht enthält die Schaltfläche **Welcome Mail erneut versenden**, um die Begrüßungs-E-Mail erneut zu senden, wenn der Benutzer die erste Welcome Mail nicht erhalten hat oder diese verloren gegangen ist.

10.3.3 Importieren von Benutzern mit der internen Benutzerverwaltung

Mit der internen Benutzerverwaltung können Sie neue Self Service Portal Benutzer hinzufügen, indem Sie eine .csv-Datei mit bis zu 300 Benutzern importieren.

Auf der Import-Seite steht eine Musterdatei mit den korrekten Spaltennamen und der richtigen Spaltenreihenfolge zum Download zur Verfügung.

Hinweis: Verwenden Sie einen Text-Editor zum Bearbeiten der .csv-Datei. Wenn Sie Microsoft Excel verwenden, werden die eingegebenen Werte u. U. nicht korrekt aufgelöst. Speichern Sie die Datei mit der Dateinamenerweiterung .csv.

Voraussetzung: Die interne Benutzerverwaltung ist für den Kunden, an dem Sie angemeldet sind, aktiviert. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service gilt. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt. Informationen darüber, wie Sie die Methoden für die Benutzerverwaltung für Sophos Mobile Control as a Service festlegen, finden Sie unter Konfigurieren der Self Service Portal Benutzerverwaltung für Sophos Mobile Control as a Service (Seite 26).

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Benutzer**.

   Die **Benutzer anzeigen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Benutzer importieren**.

   Die **Benutzer importieren** Ansicht wird angezeigt.

   Wenn Sie noch keine .csv-Datei mit Benutzern haben, können Sie nun eine Musterdatei herunterladen und diese zum Erstellen Ihrer Importdatei verwenden.

3. Stellen Sie sicher, dass das Feld **Welcome Mails versenden** ausgewählt ist.
4. Wählen Sie die zu importierende .csv-Datei aus und klicken Sie auf **Datei hochladen**.

   Die Einträge in der .csv-Datei werden auf Fehler überprüft und auf der Import-Seite angezeigt.

   Hinweis: Wenn die .csv-Datei Fehler enthält, kann sie nicht importiert werden. Neben den relevanten Einträgen wird jeweils eine Fehlermeldung angezeigt. Bearbeiten Sie die .csv-Datei entsprechend und versuchen Sie es noch einmal.

5. Wenn alle Einträge korrekt sind, klicken Sie auf die **Fertigstellen** Schaltfläche.

Die Benutzer werden importiert und in der **Benutzer anzeigen** Ansicht angezeigt.

Von der **Benutzer anzeigen** Ansicht aus können Sie die Benutzerdetails einsehen, bearbeiten und Benutzer löschen.

11 Systemeinstellungen

11.1 Überprüfen Ihrer Lizenzen

Hinweis: Sophos Mobile Control beruht auf einer benutzerbasierten Lizenzregelung. Eine einzelne Benutzerlizenz ist für alle Geräte gültig, die dem betreffenden Benutzer zugewiesen sind. Für Geräte, die keinem Benutzer zugewiesen sind, ist jeweils eine Lizenz erforderlich.

Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Setup** und dann auf **Systemeinstellungen**. Auf der Registerkarte **Lizenz** sehen Sie die Lizenzinformationen. Die Lizenzinformationen werden für die **Standardlizenz** und die **Advanced-Lizenz** separat angezeigt:

- **Anzahl von Lizenzen:**

  Zeigt die Anzahl an Endbenutzern an, die von der Web-Konsole aus verwaltet werden kann.

- **Genutzte Lizenzen:**

  Zeigt die Anzahl an genutzten Lizenzen.

- **Gültig bis:**

  Zeigt das Lizenzablaufdatum an.

Wenn Sie Fragen zu den Lizenzinformationen haben, oder wenn die angezeigten Informationen Ihrer Meinung nach nicht korrekt sind, wenden Sie sich an Ihren Sophos Vertriebspartner.

11.2 Hochladen des Apple Push Notification Keystore

Um das integrierte Mobile Device Management (MDM)-Protokoll von Geräten mit Apple iOS 4 (oder höher) verwenden zu können, muss Sophos Mobile Control den Apple Push Notification Service (APNs) zum Triggern von iOS-Geräten nutzen. Um den Apple Push Notification Service zu aktivieren, müssen Sie den Apple Push Notification Keystore in die Web-Konsole hochladen. Informationen dazu, wie Sie Ihr APNs-Zertifikat für Sophos Mobile Control erhalten, finden Sie in der *Sophos Mobile Control Startup-Anleitung* bzw. in der *Sophos Mobile Control as a Service Startup-Anleitung*.

Informationen zum Erneuern Ihres APNs-Zertifikats finden Sie unter http://www.sophos.com/de-de/support/knowledgebase/118926.aspx.

Voraussetzung: Sie haben Ihr APNs Zertifikat für Sophos Mobile Control erhalten.

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Systemeinstellungen** und gehen Sie zur Registerkarte **iOS APNS**.
2. Klicken Sie auf **Datei hochladen**. Suchen Sie nach der .P12 Zertifikatsdatei, die Sie erstellt haben und geben Sie Ihr Kennwort ein. Nach Wunsch können Sie Ihre Apple ID eingeben, falls Sie diese später benötigen.

   Wenn die Datei erfolgreich hochgeladen wurde, wird eine Bestätigungsmeldung angezeigt. Außerdem werden die Informationen zu **Topic**, **Typ** und **Ablaufdatum** Ihres APNs-Zertifikats angezeigt.

3. Klicken Sie auf **Speichern**.

11.2.1 Konfigurieren von Wiedergabegeräten für die Spiegelung per AirPlay

Mit Sophos Mobile Control können Sie das Spiegeln von Inhalten per AirPlay zwischen einem iOS-Gerät und einem vordefinierten AirPlay-Wiedergabegerät (zum Beispiel AppleTV) remote auslösen.

Hinweis: AirPlay funktioniert nur innerhalb eines Netzwerks.

Sie können die Wiedergabegeräte für die Spiegelung per AirPlay in der Web-Konsole definieren.

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Systemeinstellungen** und gehen Sie zur Registerkarte **iOS APNS**.

   Im unteren Teil der Registerkarte **iOS APNS** finden Sie den Bereich **Airplay-Wiedergabegeräte**.

2. Klicken Sie auf die Schaltfläche **Airplay-Wiedergabegerät anlegen**.

   Die **AirPlay-Wiedergabegerät** Ansicht wird angezeigt.

3. Geben Sie den **Gerätenamen** (Pflichteingabe) und die **MAC-Adresse** (optional) ein. Falls notwendig, geben Sie das **Kennwort** für das AirPlay-Wiedergabegerät ein.
4. Klicken Sie auf die **Übernehmen** Schaltfläche.

   Das Gerät wird unter **AirPlay-Wiedergabegeräte** auf der Registerkarte **iOS APNS** in der Ansicht **Systemeinstellungen** angezeigt.

5. Klicken Sie auf **Speichern**.

Sie können die Spiegelung per AirPlay zwischen einem iOS-Gerät und diesem Wiedergabegerät auslösen, indem Sie in der Ansicht **Gerät anzeigen** oder **Gerät bearbeiten** für das gewünschte Gerät im Menü **Aktionen** auf die Schaltfläche **AirPlay-Wiedergabe anfordern** klicken.

11.3 Konfigurieren eines VPP-Service-Token (sToken)

Um die Lizenzen für über das Apple Volume Purchase Program erworbene Apps in Sophos Mobile Control zur Verfügung zu stellen, müssen Sie in der Web-Konsole einen VPP-Service-Token konfigurieren.

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Setup** und dann auf **Systemeinstellungen**.

   Die **Systemeinstellungen** Ansicht wird angezeigt.

2. Klicken Sie auf der Registerkarte **Apple Volume Purchase Program** auf **Datei hochladen**. Suchen Sie nach der Service Token-Datei (.vpptoken), wählen Sie diese aus und klicken Sie auf **Öffnen**.

   Organisation und **Ablaufdatum** werden automatisch von der importierten Datei übernommen.

3. Geben Sie optional Ihre Apple-ID und den Ländercode ein.
4. Klicken Sie auf die **Speichern** Schaltfläche.

Hinweis: Wenn Sie Ihre Änderungen gespeichert haben wird der Text des Service Token aus Sicherheitsgründen nicht mehr im Textfeld angezeigt. Das Feld zeigt jedoch, dass ein Service Token konfiguriert ist.

11.4 Konfigurieren von SCEP für iOS-Geräte

Für iOS-Geräte können Sie das Simple Certificate Enrollment Protocol (SCEP) für die Bereitstellung der Zertifikate konfigurieren. Auf diese Weise können Geräte Zertifikate über SCEP bei einer Zertifizierungsstelle beziehen.

Sie können alle Einstellungen festlegen, die für den Zugriff auf einen CA-Server über SCEP in der Web-Konsole erforderlich sind.

Sie können die für die Geräte erforderlichen Einstellungen in den iOS SCEP-Konfigurationen festlegen.

11.4.1 Voraussetzungen

Um den Simple Certificate Enrollment Process nutzen zu können, müssen die folgenden Voraussetzungen erfüllt sein:

- In der Umgebung muss eine SCEP-fähige Windows-CA vorhanden sein.
- Die Anmeldedaten für einen Benutzer, der einen Challange-Code erstellen kann, sind verfügbar.
- Der Sophos Mobile Control Server hat http- oder https-Zugriff auf die folgenden Websites:
  - https://YOUR-SCEP-SERVER/CertSrv/MSCEP_ADMIN
  - https://YOUR-SCEP-SERVER/CertSrv/MSCEP

11.4.2 Konfigurieren der SCEP-Einstellungen

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Systemeinstellungen** und gehen Sie zur Registerkarte **SCEP**.
2. Machen Sie die folgenden Angaben:
   a) Geben Sie im Feld **SCEP Server URL** https://YOUR-SCEP-SERVER/CertSrv/MSCEP ein.
   b) Geben Sie im Feld **Challenge URL** https://YOUR-SCEP-SERVER/CertSrv/MSCEP_ADMIN ein.

      Hinweis: Wenn Sie einen Windows 2003-Server als SCEP-Server verwenden, geben Sie https://YOUR-SCEP-SERVER/CertSrv/MSCEP ein.

   c) Geben Sie in den Feldern **Benutzer** und **Kennwort** die Zugangsdaten des Benutzers ein, der einen Challenge-Code erstellen kann.

      Hinweis: Geben Sie im Feld **Benutzer** einen Benutzer ein, der über die erforderlichen Berechtigungen für die Bereitstellung von Zertifikaten verfügt. Verwenden Sie das folgende Anmeldeformat: username@domain

   d) Akzeptieren Sie im Feld **Challenge-Länge** die Standardlänge.
3. Klicken Sie auf die **Speichern** Schaltfläche.

   Sophos Mobile Control testet die Verbindung zum SCEP-Server.

Es besteht jetzt eine funktionierende Verbindung zu Ihrem SCEP-Server. Um ein Profil über SCEP bereitzustellen, müssen Sie ein iOS-Profil erstellen, wie im nächsten Schritt beschrieben.

11.4.3 Konfigurieren eines SCEP iOS-Profils

1. Erstellen Sie ein neues iOS-Profil und geben Sie die erforderlichen allgemeinen Informationen ein.
2. Klicken Sie auf **Hinzufügen**.

   Die **Verfügbare Konfigurationen** Ansicht wird angezeigt.

3. Wählen Sie in der Liste der verfügbaren Konfigurationen **SCEP** aus.

   Die Ansicht **SCEP** wird angezeigt.

4. Akzeptieren Sie im Feld **URL** den Standardwert. Dieser sollte %_SCEPPROXYURL_% lauten.
5. Geben Sie in das Feld **CA-Name** den Namen der Zertifizierungsstelle ein.
6. Im Feld **Betreff** können Sie den Namen der Person eingeben, die das Zertifikat erhält. Stellen Sie dem eigentlichen Namen/Wert „CN=“ voran. Sie können die verfügbaren LDAP-Variablen verwenden, z. B. „CN=%_USERNAME_%“.
7. Lassen Sie das Feld **Challenge** unverändert.
8. Stellen Sie sicher, dass der im Feld **Schlüsselgröße** festgelegte Wert der auf dem SCEP-Server konfigurierten Größe entspricht.
9. Konfigurieren Sie die übrigen Felder entsprechend den Erfordernissen und klicken Sie auf **Übernehmen**.

   Die Ansicht **Profil bearbeiten** wird wieder angezeigt.

10. Klicken Sie auf **Speichern**.

Sie können jetzt Profile beispielsweise für WLAN oder VPN hinzufügen und das Zertifikat/die Zertifizierungsstelle als Authentifizierungsmethode auswählen. Das Zertifikat für Ihr Gerät wird erzeugt, sobald das Profil bereitgestellt wurde.

11.5 Konfigurieren des Benutzerverzeichnisses

Auf der Registerkarte **Benutzerverzeichnis** können Sie die Einstellungen für die Benutzerverwaltung ändern. Weitere Informationen finden Sie unter Verwalten von Self Service Portal Benutzern (Seite 26) und im Sophos Mobile Control Super Administrator Guide.

11.6 Samsung Knox-Lizenz

Wenn Ihr Unternehmen eine gültige Samsung Knox-Lizenz besitzt, müssen Sie Ihren Lizenzschlüssel, die Anzahl der Lizenzen und das Ablaufdatum auf der Registerkarte **Samsung Knox-Lizenz** eingeben, damit Sie Ihre Knox-Geräte mit Sophos Mobile Control verwalten können.

12 Konfigurieren von Geräterichtlinien

In der Sophos Mobile Control Web-Konsole können Sie:

- Geräterichtlinien für alle verfügbaren Gerätetypen (Plattformen) definieren.
- Aktionen festlegen, die ausgeführt werden, wenn Geräte nicht mehr den festgelegten Regeln entsprechen.
- Mehrere Geräterichtlinien definieren und diese Gerätegruppen zuweisen. In Gerätegruppen können Sie unterschiedliche Geräterichtlinien für Firmengeräte und private Geräte auswählen. Somit können Sie auf Unternehmens- und private Geräte unterschiedliche Sicherheitsstufen anwenden.

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Geräterichtlinien**.

   Die **Geräterichtlinien** Listenansicht wird angezeigt.

2. Klicken Sie auf **Richtlinien anlegen**.
3. Die **Geräterichtlinien** Ansicht mit Registerkarten für alle verfügbaren Gerätetypen wird angezeigt.
4. Geben Sie einen **Namen** und eine **Beschreibung** für die neue Geräterichtlinie ein.
5. Wechseln Sie in die erforderliche Registerkarte.
6. Stellen Sie sicher, dass das Feld **Plattform aktivieren** ausgewählt ist.

   Hinweis: Wenn dieses Feld nicht ausgewählt ist, können die Geräte der Plattform nicht auf Compliance überprüft werden.

7. Konfigurieren Sie unter **Regel** die Compliance-Anforderungen für den ausgewählten Gerätetyp. Eine Auflistung der für die einzelnen Gerätetypen verfügbaren Einstellungen finden Sie unter Verfügbare Geräterichtlinien (Seite 36).
8. Unter **Active Sync sperren** können Sie festlegen, dass der E-Mail-Zugriff automatisch verweigert wird, wenn Geräte nicht den Richtlinien entsprechen. Wählen Sie die erforderlichen Kontrollkästchen neben den entsprechenden Regeln aus.
9. Unter **Netzwerkzugriff sperren** können Sie festlegen, dass der Netzwerkzugriff automatisch verweigert wird, wenn Geräte nicht den Richtlinien entsprechen. Wählen Sie die erforderlichen Kontrollkästchen neben den entsprechenden Regeln aus.

   Dieses Feld wird nur dann angezeigt, wenn Network Access Control für den Kunden konfiguriert ist. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

10. Unter **Dokumentenzugriff sperren** können Sie festlegen, dass der Zugriff auf verschlüsselte Dokumente automatisch verweigert wird, wenn Geräte nicht den Richtlinien entsprechen. Benutzer können die Sophos Secure Workspace App nicht mehr verwenden. Wählen Sie die erforderlichen Kontrollkästchen neben den entsprechenden Regeln aus.

    Hinweis: Diese Spalte wird nur angezeigt, wenn eine SMC Advanced-Lizenz für die Verwaltung von Sophos Secure Workspace verfügbar ist.

11. Unter **Admin benachrichtigen** können Sie festlegen, dass Administratoren per E-Mail benachrichtigt werden, wenn Geräte nicht den Compliance-Richtlinien entsprechen. Wählen Sie die erforderlichen Kontrollkästchen neben den entsprechenden Regeln aus.

12. Unter **Auftragspaket übertragen** können Sie Auftragspakete auswählen, die für die entsprechenden **Regel** Einstellungen übertragen werden. Wenn Geräte nicht mit den Regeln übereinstimmen, werden die ausgewählten Auftragspakete automatisch übertragen.

    Hinweis: Sie müssen die Auftragspakete zuerst in der Web-Konsole anlegen. Wenn Sie noch kein Auftragspaket erstellt haben, aktualisieren Sie die Geräterichtlinien danach. Informationen zum Erstellen eines Auftragspakets finden Sie unter Mit Auftragspaketen arbeiten (Seite 104).

13. Wenn Sie alle Einstellungen in allen erforderlichen Gerätetyp-Registerkarten konfiguriert haben, klicken Sie auf die **Speichern** Schaltfläche.

    Die neue Geräterichtlinie wird in der **Geräterichtlinien** Listenansicht angezeigt.

14. Wenn Sie festgelegt haben, dass Administratoren per E-Mail benachrichtigt werden sollen, wenn Geräte nicht mehr die Compliance-Regeln erfüllen, geben Sie die gewünschten Empfänger unter **Compliance-E-Mail Empfänger** an. Verwenden Sie zum Trennen mehrerer Empfänger das Semikolon (**;**). Legen Sie unter **Compliance-E-Mail Zeitplan** einen Zeitplan für die Benachrichtigung fest.
15. Klicken Sie auf die **Speichern** Schaltfläche.

Die neue Geräterichtlinie kann Gerätegruppen zugewiesen werden. In Gerätegruppen können Sie unterschiedliche Geräterichtlinien für Firmengeräte und private Geräte auswählen.

12.1 Verfügbare Geräterichtlinien

Die folgende Tabelle zeigt die Geräterichtlinien, die Sie für die einzelnen Plattformen unter **Regel** auf der betreffenden Registerkarte **Geräterichtlinien** auswählen können.

Einstellung	Beschreibung	Android	iOS	Windows Phone 8
Min. Client-Version	Geben Sie die Sophos Mobile Control Client Mindestversion ein, die auf dem Gerät installiert sein muss.	✓	✓	✓
Root-Rechte erlauben	Wählen Sie aus, ob Geräte mit Root-Rechten zulässig sind.	✓	✗	✗
Jailbreak erlauben	Wählen Sie aus, ob Jailbroken-Geräte zulässig sind.	✗	✓	✗
Kennwort erforderlich	Wählen Sie aus, ob für Geräte ein Kennwort erforderlich ist.	✗	✓	✓
Non-Market Apps erlauben	Wählen Sie aus, ob Non-Market Apps auf Geräten zulässig sind.	✓	✗	✗

Einstellung	Beschreibung	Android	iOS	Windows Phone 8
Debug Bridge (ADB) erlauben	Wählen Sie aus, ob ADB (Android Debug Bridge) auf Geräten zulässig ist.	✓	✗	✗
Min. OS-Version:	Wählen Sie die Mindestversion für das Betriebssystem auf Geräten aus.	✓	✓	✓
Max. OS-Version:	Wählen Sie die Maximalversion für das Betriebssystem auf Geräten aus.	✓	✓	✓
Max. Synchronisationsabstand	Geben Sie das maximale Intervall zwischen Synchronisierungsvorgängen für Geräte an.	✓	✓	✓
Max. Synchronisationsabstand der SMC-App	Geben Sie das maximale Intervall zwischen iOS App-Synchronisierungsvorgängen für Geräte an. Weitere Informationen finden Sie im *Sophos Mobile Control Benutzerhandbuch für Apple iOS*. **Hinweis:** Diese Einstellung betrifft nur Geräte mit einer älteren iOS-Version als iOS 7. Bei iOS 7-Geräten hat sie keine Auswirkungen.	✗	✓	✓
Max. SMSec-Scanintervall	Dieses Feld wird nur dann angezeigt, wenn für den Kunden Sophos Mobile Security verfügbar ist. Für weitere Informationen siehe Verwaltung von Sophos Mobile Security über Sophos Mobile Control (Seite 126). In diesem Feld können Sie den Höchstabstand zwischen Malware Scans angeben, die von der Sophos Mobile Security App auf dem Gerät durchgeführt werden.	✓	✗	✗

Einstellung	Beschreibung	Android	iOS	Windows Phone 8
Malware Apps zugelassen	Dieses Feld wird nur dann angezeigt, wenn für den Kunden Sophos Mobile Security verfügbar ist. Wählen Sie aus, ob Malware Apps auf Geräten zulässig sind.	✓	✗	✗
Verdächtige Apps zugelassen	Dieses Feld wird nur dann angezeigt, wenn für den Kunden Sophos Mobile Security verfügbar ist. Wählen Sie aus, ob verdächtige Apps auf Geräten zulässig sind.	✓	✗	✗
PUA zugelassen	Dieses Feld wird nur dann angezeigt, wenn für den Kunden Sophos Mobile Security verfügbar ist. Wählen Sie aus, ob PUAs (Potentially Unwanted Apps) auf Geräten zulässig sind.	✓	✗	✗
Hardwareverschlüsselung erforderlich	Wählen Sie aus, ob für Geräte Verschlüsselung erforderlich ist.	✓	✓	✓
Data-Roaming erlaubt	Wählen Sie aus, ob für Geräte Daten-Roaming zulässig ist.	✓	✓	✓
App-Lokalisierung erforderlich	Diese Einstellung bezieht sich auf die **Lokalisieren** Funktion für iOS-Geräte. Legen Sie fest, ob der Benutzer der Sophos Mobile Control App gestatten muss, Ortsdaten abzurufen, damit das Gerät richtlinienkonform ist.	✗	✓	✓
Erforderliche Apps	Geben Sie Apps an, die auf den Geräten installiert werden müssen. Klicken Sie auf **Bearbeiten**. Fügen Sie in der **Erforderliche Apps** Ansicht die App(s) hinzu, die Sie als erforderlich definieren möchten, und klicken Sie auf **Übernehmen**.	✓	✓	✗

12.2 Zuweisen von Geräterichtlinien zu Gerätegruppen

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Gerätegruppen**.

   Die **Gerätegruppen** Ansicht wird angezeigt.

2. Klicken Sie auf das blaue Dreieck neben der Gerätegruppe, der Sie Geräterichtlinien zuweisen möchten, und klicken Sie auf **Bearbeiten**.

   In der Web-Konsole steht eine **Default** Gerätegruppe zur Verfügung. Für weitere Informationen zum Erstellen eigener Gerätegruppen siehe Erstellen von Gerätegruppen (Seite 40).

3. Wählen Sie unter **Geräterichtlinien** in den Feldern für **Firmengeräte** und für **private Geräte** die Geräterichtlinien, die Sie anwenden möchten.
4. Klicken Sie auf die **Speichern** Schaltfläche.

Die ausgewählten Geräterichtlinien werden in der Ansicht **Gerätegruppen** für die jeweilige Gerätegruppe unter **Richtlinie für Firmengeräte** und **Richtlinie für private Geräte** angezeigt.

12.3 Compliance-Prüfung bei Geräten

Wenn Sie Compliance-Einstellungen definiert haben, können Sie prüfen, ob registrierte Geräte den definierten Richtlinien entsprechen.

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Geräterichtlinien**.

   Die **Compliance-Einstellungen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Jetzt prüfen**.

Alle registrierten Geräte werden nach den unter **Compliance-Einstellungen** definierten Regeln geprüft. Die festgelegten Aktionen werden ausgeführt. Das Tortendiagramm auf der **Startseite** wird entsprechend aktualisiert.

13 Hinzufügen von Geräten zu Sophos Mobile Control

Es gibt folgende Möglichkeiten, um Geräte zur Sophos Mobile Control Web-Konsole hinzuzufügen:

- Manuelles Hinzufügen von Geräten in der Web-Konsole
- Importieren von Geräten in einer .csv-Datei in der Web-Konsole
- Berechtigen von Benutzern zur Registrierung ihrer eigenen Geräte über das Self Service Portal. Siehe Konfigurieren der Benutzung des Self Service Portal für Endbenutzer (Seite 22). Dieses Portal verringert den Aufwand für die IT, weil die Benutzer Aufgaben ausführen können, ohne sich an das Helpdesk wenden zu müssen. Die Geräte werden durch Ausführen vordefinierter Auftragspakete provisioniert (siehe Mit Auftragspaketen arbeiten (Seite 104)).

  Weitere Informationen zur Nutzung des Self Service Portal für die Registrierung von Geräten finden Sie im *Sophos Mobile Control Benutzerhandbuch.*

Zur Vereinfachung der Verwaltung lassen sich Geräte gruppieren. Sie können Geräte vorhandenen Gerätegruppen zuordnen, wenn Sie sie zur Sophos Mobile Control Web-Konsole hinzufügen. In der Web-Konsole steht eine **Default** Gerätegruppe zur Verfügung. Wenn Sie noch keine eigenen Gerätegruppen definiert haben, können Sie Geräte zu dieser Gruppe hinzufügen.

13.1 Erstellen von Gerätegruppen

Wir empfehlen, Geräte zu gruppieren. Da sich Aufgaben auch bei Gerätegruppen statt bei Einzelgeräten ausführen lassen, können Sie Geräte so effizient verwalten.

Hinweis: Wir empfehlen, nur Geräte mit demselben Betriebssystem zu gruppieren. Gruppen lassen sich dadurch leichter für Installationen und andere betriebssystemspezifische Vorgänge verwenden.

So erstellen Sie eine neue Gerätegruppe:

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Gerätegruppen**.

   Die **Gerätegruppen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Gerätegruppe anlegen**.

   Die **Gerätegruppe bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Beschreibung** für die neue Gerätegruppe ein.
4. Wählen Sie unter **Geräterichtlinien** in den Feldern **für Firmengeräte** und **für private Geräte** die Geräterichtlinien, die Sie anwenden möchten.
5. Klicken Sie auf die **Speichern** Schaltfläche.

   Hinweis: Die Einstellungen für die Gerätegruppen enthalten die Option **Enable auto-enrollment**. Mit dieser Option können Sie iOS-Geräte mit dem Apple Configurator bereitstellen.

Die neue Gerätegruppe wird angelegt und in der **Gerätegruppen** Ansicht angezeigt. Sie können nun Geräte zur neuen Gruppe hinzufügen.

Hinweis: Wenn Sie eine Gerätegruppe löschen, werden die Mitglieder der Gruppe in eine andere Gruppe verschoben. Diese muss angegeben werden. Ist keine Gruppe mehr vorhanden, in die die Geräte verschoben werden können, so kann die Gruppe nicht gelöscht werden. Bevor eine Gruppe gelöscht wird, wird eine Warnungsmeldung angezeigt.

13.2 Erstellen eines neuen Geräts

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die **Geräte** Ansicht wird angezeigt.

2. Klicken Sie auf **Gerät anlegen** und wählen Sie den Gerätetyp aus.

   Die **Gerät bearbeiten** Ansicht wird angezeigt.

3. Geben Sie in der **Gerät bearbeiten** Ansicht die folgenden Gerätedetails an:

   a) Geben Sie im Feld **Name** einen eindeutigen Namen für das neue Gerät ein.

   b) Geben Sie im Feld **Beschreibung** eine Beschreibung für das neue Gerät ein.

   c) Wählen Sie unter **Eigentümer** die Option **Firmengerät** oder **Privates Gerät**.

   d) Geben Sie im Feld **E-Mail-Adresse** eine E-Mail-Adresse ein.

      Hinweis: Pflichtfelder sind mit einem roten Sternchen (*) markiert.

   e) Geben Sie im **Telefonnummer** Feld die Telefonnummer des neuen Geräts ein. Dieses Feld ist ein Pflichtfeld. Wenn Sie ein Gerät hinzufügen, das keine Telefonnummer hat (zum Beispiel ein Tablet), geben Sie hier 0 ein. Geben Sie die Telefonnummer in internationalem Format an, zum Beispiel: "+491701234567".

   f) Wählen Sie unter **Gerätegruppe** die Gerätegruppe, zu der das Gerät hinzugefügt werden soll.

      Hinweis: Hier steht eine **Default** Gerätegruppe zur Verfügung. Wenn Sie noch keine eigenen Gerätegruppen definiert haben, können Sie Geräte zu dieser Gruppe hinzufügen. Für weitere Informationen zum Erstellen eigener Gerätegruppen siehe Erstellen von Gerätegruppen (Seite 40).

4. Um einen LDAP-Link zum Gerät hinzuzufügen, klicken Sie auf die Schaltfläche **Aktionen** und dann auf **Benutzer zuordnen**. Weitere Informationen finden Sie unter Zuweisen eines Benutzers zu einem Gerät (Seite 118).
5. Um eigene Eigenschaften zum Gerät hinzuzufügen, wechseln Sie in die **Eigene Eigenschaften** Registerkarte und klicken Sie auf die **Eigenschaft anlegen** Schaltfläche. Für weitere Informationen siehe Definieren eigener Eigenschaften für Geräte (Seite 119).
6. Wenn Sie alle erforderlichen Gerätedetails angegeben haben, klicken Sie auf die **Speichern** Schaltfläche.

Das neue Gerät wird zur Sophos Mobile Control Web-Konsole hinzufügt und in der Ansicht **Geräte** unter **VERWALTEN** angezeigt. Sie können das Gerät nun provisionieren und verwalten.

13.3 Duplizieren eines Geräts

Sie können in Sophos Mobile Control neue Geräte durch Duplizieren bereits vorhandener Geräte anlegen.

Hinweis: Sie können nur Geräte duplizieren, die nicht gerade bearbeitet werden. Die Kopien werden mit "Copy of" und dem Namen des Originalprofils benannt. Sie können die Namen der Geräte nach Ihren Anforderungen ändern.

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die **Geräte** Ansicht wird angezeigt.

2. Klicken Sie auf das Gerät, das Sie duplizieren wollen.

   Die **Gerät anzeigen** Ansicht wird angezeigt.

3. Klicken Sie auf die Schaltfläche **Aktionen** und dann auf **Dieses Gerät duplizieren**.

Das Gerät wird dupliziert und in der **Geräte** Ansicht angezeigt. Sie können das duplizierte Gerät nun bearbeiten. Um das Gerät zu bearbeiten, klicken Sie auf das daneben stehende blaue Dreieck und dann auf **Bearbeiten**.

13.4 Importieren von Geräten

Sie können neue Geräte durch Import einer .csv-Datei mit bis zu 500 Geräten hinzufügen. In der **Geräte importieren** Ansicht steht eine Musterdatei mit den korrekten Spaltennamen und der richtigen Spaltenreihenfolge zum Download zur Verfügung.

Hinweis: Verwenden Sie einen Text-Editor zum Bearbeiten der .csv-Datei. Wenn Sie Microsoft Excel verwenden, werden die eingegebenen Werte u. U. nicht korrekt aufgelöst. Speichern Sie die Datei mit der Dateinamenerweiterung .csv.

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die **Geräte** Ansicht wird angezeigt.

2. Klicken Sie auf **Geräte importieren**.

   Die **Geräte importieren** Ansicht wird angezeigt.

   Hinweis: Wenn Sie noch keine .csv-Datei mit Geräten haben, können Sie nun eine Musterdatei herunterladen und diese zum Erstellen Ihrer Importdatei verwenden.

3. Klicken Sie auf **Datei hochladen** und suchen Sie nach der .csv-Datei. Wählen Sie diese aus und klicken Sie auf **Öffnen**.

   Die Einträge in der .csv-Datei werden auf Fehler überprüft und auf der Import-Seite angezeigt.

   Hinweis: Wenn die .csv-Datei Fehler enthält, kann sie nicht importiert werden. Neben den relevanten Einträgen wird jeweils eine Fehlermeldung angezeigt. Bearbeiten Sie die .csv-Datei entsprechend und versuchen Sie es noch einmal.

4. Wenn alle Einträge korrekt sind, klicken Sie auf die **Fertigstellen** Schaltfläche.

Die in der .csv-Liste aufgelisteten Geräte werden importiert und in der **Geräte** Ansicht angezeigt. Sie können die Geräte nun provisionieren und verwalten.

14 Samsung Knox-Unterstützung

Sie können Ihre Samsung Knox-Geräte über die Sophos Mobile Control Web-Konsole verwalten.

Hinweis: Zur Verwaltung von Samsung Knox-Geräten muss ein Samsung **Knox Advanced-Lizenzschlüssel** in den Sophos Mobile Control **Systemeinstellungen** eingegeben werden.

Unter **Profile** können Sie ein Profil erstellen, das die Einstellungen für den Knox-Container enthält. Die folgenden Konfigurationen sind verfügbar:

- **Kennwortrichtlinien**
- **Einschränkungen**
- **Exchange Active Sync**

Informationen zum Erstellen eines Profils für ein Knox-Gerät finden Sie unter Erstellen von Container-Profilen für Android-Geräte (Seite 61).

Sie können Apps hochladen oder einen Link zu Apps bereitstellen und diese in einem Knox-Container installieren (siehe Hochladen von Apps zur Web-Konsole (Seite 106) und Anlegen von Links zu Apps (Seite 107)).

Zur Verwaltung Ihrer KNOX-Geräte können Sie Auftragspakete für die folgenden Aktionen erstellen:

- **Container: Sperren**
- **Container: Entsperren**
- **Container: Kennwort zurücksetzen**
- **Container: Alle Einstellungen entfernen**

Informationen zum Erstellen eines Auftragspakets für ein Knox-Gerät finden Sie unter Erstellen von Auftragspaketen (Seite 104).

15 Mit Profilen arbeiten

In der Web-Konsole können Sie unter **Profile** Einstellungsprofile für Apple iOS-, Android- und Windows Phone 8-Geräte erstellen und übertragen.

Für iOS-Geräte können Sie auch Profile hochladen, die mit der iPhone Configuration Utility erstellt wurden, und diese an Geräte übertragen.

Für Windows Mobile-Geräte können Sie Vorlagen für Einstellungsprofile verwalten. Diese definieren die Einstellungsoptionen, die für die Benutzer der Web-Konsole zur Verfügung stehen. Die Vorlagen werden von Sophos zur Verfügung gestellt.

Hinweis: Bei Android-Geräten richten sich die Einstellungen nach herstellerspezifischen APIs. Je nach Endbenutzergerät haben einige Einstellungen unter Umständen keine Auswirkung. Weitere Informationen finden Sie in der Feature Matrix im *Sophos Mobile Control Technical Guide* (Englisch).

15.1 Erstellen von Geräteprofilen für Android-Geräte

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Profile** und dann auf **Android**.

   Die **Profile** Ansicht wird angezeigt.

2. Klicken Sie auf **Profil anlegen** und wählen Sie **Geräteprofil anlegen**.

   Die **Profil bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Version** für das neue Profil ein.
4. Geben Sie im Feld **Beschreibung** eine Beschreibung für das Profil ein.
5. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das das Profil gelten soll.
6. Klicken Sie auf die Schaltfläche **Konfiguration hinzufügen**.

   Die **Verfügbare Konfigurationen** Ansicht wird angezeigt.

7. Wählen Sie die Konfiguration aus, die Sie hinzufügen möchten, und klicken Sie auf **Weiter**.

   Die Einstellungen-Ansicht der Konfiguration wird angezeigt.

8. Definieren Sie die erforderlichen Einstellungen. Für eine detaillierte Liste aller verfügbaren Konfigurationen und Einstellungen siehe Verfügbare Android-Konfigurationen (Seite 44).
9. Klicken Sie auf die **Übernehmen** Schaltfläche, um Ihre Änderungen zu speichern.

   Die Konfiguration wird in der **Profil bearbeiten** Ansicht unter **Konfigurationen** angezeigt.

10. Wenn Sie alle erforderlichen Konfigurationen hinzugefügt haben, klicken Sie auf die **Speichern** Schaltfläche.

Das Profil steht für die Übertragung zur Verfügung. Es wird in der Ansicht **Profile** für **Android** angezeigt.

15.1.1 Verfügbare Android-Konfigurationen

Die folgenden Konfigurationen sind für Android-Profile in der **Verfügbare Konfigurationen** Ansicht verfügbar, wenn Sie ein Profil erstellen oder bearbeiten. Einige Konfigurationen lassen sich in einem Profil nur einmal hinzufügen, andere mehrmals.

Hinweis: Die unterstützten Einstellungen hängen von anbieterspezifischen APIs und von der Android-Version ab, die auf den einzelnen Geräten in Gebrauch ist. Je nach Endbenutzergerät haben einige Einstellungen unter Umständen keine Auswirkung. In den einzelnen Konfigurationen wird in der Web-Konsole durch entsprechende Information darauf hingewiesen, ob eine Einstellung nur für eine bestimmte Android-Version oder nur für Geräte mit Samsung Safe-Plugin (zum Beispiel **SAFEv2+**) oder mit aktivem TouchDown E-Mail-Client (**TouchDown**) unterstützt wird. In den folgenden Beschreibungen der Einstellungen finden Sie diese Informationen jeweils wie erforderlich zu Beginn der einzelnen Abschnitte oder in einer Tabellenspalte zu den geltenden Mindestanforderungen.

Kennwortrichtlinien

In dieser Konfiguration können Sie Kennwortrichtlinien für Geräte definieren. Sie können nur eine **Kennwortrichtlinien** Konfiguration in einem Profil hinzufügen.

Wenn Sie die **Kennwortrichtlinien** Konfiguration auswählen, wird das **Kennworttyp** Feld angezeigt. Wählen Sie in diesem Feld die Art des Kennworts, dass Sie definieren möchten:

- **Beliebig**

  Wenn Sie diese Einstellung wählen, müssen Benutzer ein Kennwort auf dem Endgerät einstellen. Für das Kennwort gelten jedoch keine Anforderungen oder Einschränkungen. Wenn Sie diese Option wählen, sind für die **Kennwortrichtlinien** Konfiguration keine weiteren Einstellungen erforderlich.

- **Alphabetisch**
- **PIN**
- **Alphanumerisch**
- **Komplex**

Wenn Sie **Alphabetisch**, **PIN** oder **Alphanumerisch** auswählen, werden die folgenden Felder angezeigt:

Einstellung/Feld	Beschreibung
Minimale Länge des Kennworts	Gibt an, wie viele Zeichen ein Kennwort mindestens enthalten muss.
Inaktivitätszeit in Sekunden bis zur Abfrage des Kennworts	In diesem Feld können Sie festlegen, wann (in Sekunden) das Gerät nach Nichtbenutzung gesperrt werden soll. Das Gerät lässt sich durch Eingabe des Kennworts entsperren.
Gültigkeitsdauer des Kennworts (Tage)	Fordert eine Änderung des Kennworts im angegebenen Intervall (in Tagen).
Maximale Anzahl fehlerhafter Loginversuche, bis das Gerät zurückgesetzt wird	In diesem Feld können Sie die Höchstanzahl an fehlgeschlagenen Eingabeversuchen für das Kennwort eingeben. Nach Erreichen der Höchstanzahl wird das Gerät zurückgesetzt.
Anzahl der letzten Kennwörter, die nicht benutzt werden dürfen	In diesem Feld können Sie festlegen, wie viele alte Kennwörter gespeichert und mit neu definierten

Einstellung/Feld	Beschreibung
	Kennwörtern verglichen werden. Wenn ein Benutzer ein neues Kennwort festlegt, wird es nicht akzeptiert, wenn es mit einem bereits benutzten Kennwort übereinstimmt. Wertebereich: 1 bis 5 oder kein Wert.

Wenn Sie **Komplex** auswählen, werden zusätzlich zu den für die anderen Kennworttypen angezeigten Felder die folgenden Felder angezeigt:

Einstellung/Feld	Beschreibung
Minimale Anzahl an Buchstaben	Gibt an, wie viele Buchstaben ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Kleinbuchstaben	Gibt an, wie viele Buchstaben ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Großbuchstaben	Gibt an, wie viele Buchstaben ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Zeichen, die kein Buchstabe sind	Gibt an, wie viele nicht-alphabetische Zeichen (zum Beispiel & oder !) ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Zahlen	Gibt an, wie viele Buchstaben ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Sonderzeichen	Gibt an, wie viele Sonderzeichen (zum Beispiel !"§$%&/()=,.-;:_@<>) ein Kennwort mindestens enthalten muss.

Einschränkungen

In dieser Konfiguration können Sie Einschränkungen für Geräte definieren. Sie können nur eine **Einschränkungen** Konfiguration in einem Profil hinzufügen.

Einstellung/Feld	Beschreibung	Mindestanforderungen
Verschlüsselung erzwingen		
Kamera erlauben	Wenn Sie diese Option deaktivieren, werden Kameras vollständig auf den Geräten deaktiviert.	**SAFEv2+** oder **4.0+**

Einstellung/Feld	Beschreibung	Mindestanforderungen
Kamera auf Sperrbildschirm erlauben		
Widgets auf Sperrbildschirm erlauben		
Auf Werkseinstellungen zurücksetzen erlauben	Wenn Sie diese Option deaktivieren, können Benutzer Ihre Geräte nicht auf die Werkseinstellungen zurücksetzen.	**SAFEv2+**
Einstellungen ändern erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Einstellungen auf ihren Geräten ändern. Je nach Gerät wird das Symbol für die Einstellungen entfernt.	**SAFEv2+**
Backup erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine System-Backups erstellen. Google Backup wird deaktiviert. Andere Backup-Verfahren (zum Beispiel Sophos Mobile Control Backups) bleiben aktiv.	**SAFEv2+**
Nativen Browser erlauben	Wenn Sie diese Option deaktivieren, werden native Browser auf den Geräten deaktiviert.	**SAFEv2+**
Kamera auf Sperrbildschirm erlauben	Wenn Sie diese Option deaktivieren, werden Kameras bei gesperrtem Bildschirm deaktiviert.	**4.2+**
Widgets auf Sperrbildschirm erlauben	Wenn Sie diese Option deaktivieren, werden Widgets bei gesperrtem Bildschirm deaktiviert.	**4.2+**
Zwischenablage erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Inhalte in die Zwischenablage kopieren. **Hinweis:** Diese Einstellungen gilt für Geräte ab Android 4.2.2.	**SAFEv2+**
Play Store erlauben	Wenn Sie diese Option deaktivieren, wird der Play Store auf den Geräten deaktiviert. **Hinweis:** Diese Einstellungen gilt für Geräte ab Android 4.2.2.	**SAFEv2+**
Non-Market Apps erlauben	Wenn Sie diese Option deaktivieren, werden nicht-Market Apps auf den Geräten deaktiviert.	**SAFEv2+**

Einstellung/Feld	Beschreibung	Mindestanforderungen
Bluetooth erlauben	Wenn Sie diese Option deaktivieren, wird Bluetooth auf den Geräten deaktiviert.	**SAFEv2+**
NFC erlauben	Wenn Sie diese Option deaktivieren, wird NFC (Near Field Communication) auf den Geräten deaktiviert.	**SAFEv2+**
Screenshot erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Screenshots vom Display erstellen.	**SAFEv2+**
SD-Karte erlauben	Wenn Sie diese Option deaktivieren, können in den Geräten keine SD-Karten verwendet werden.	**SAFEv2+**
USB-Debuggen erlauben	Wenn Sie diese Option deaktivieren, wird USB-Debuggen auf den Geräten deaktiviert.	**SAFEv2+**
USB erlauben	Wenn Sie diese Option deaktivieren, werden der USB-Speichermodus und der USB Media Player auf den Geräten deaktiviert.	**SAFEv2+**
WiFi-Tethering erlauben	Wenn Sie diese Option deaktivieren, wird WiFi-Tethering auf den Geräten deaktiviert.	**SAFEv2+**
USB-Tethering erlauben	Wenn Sie diese Option deaktivieren, wird USB-Tethering auf den Geräten deaktiviert.	**SAFEv2+**
Bluetooth-Tethering erlauben	Wenn Sie diese Option deaktivieren, wird Bluetooth-Tethering auf den Geräten deaktiviert.	**SAFEv2+**
Synchronisation im Roamingmodus erlauben	Wenn Sie diese Option deaktivieren, ist die Synchronisierung im Roamingmodus deaktiviert.	**SAFEv3+**
Datenverbindungen im Roamingmodus erlauben	Wenn Sie diese Option deaktivieren, sind mobile Datenverbindungen im Roamingmodus deaktiviert.	**SAFEv2+**
Home-Taste erlauben		**SAFEv2+**
Mikrofon erlauben		**SAFEv2+**
Mock GPS-Standorte erlauben		**SAFEv2+**

Einstellung/Feld	Beschreibung	Mindestanforderungen
Optionen zum Verschieben auf SD-Karte in den Geräteeinstellungen erlauben		**SAFEv5+**
Schreiben auf SD-Karte erlauben		**SAFEv5+**
Tethering erlauben		**SAFEv2+**
USB-Media Player erlauben		**SAFEv2+**
Sprachanrufe im Roamingmodus erlauben	Wenn Sie diese Option deaktivieren, sind mobile Sprachanrufe im Roamingmodus deaktiviert.	**SAFEv3+**
Versand von Crash-Reports erlauben	Wenn Sie diese Option deaktivieren, sind Crash-Reports für Applikationen deaktiviert.	**SAFEv3+**
Over-the-air Firmeware-Updates erlauben		**SAFEv3+**
Erweiterung der Statusleiste erlauben		**SAFEv4+**
Videoaufnahmen erlauben		**SAFEv4+**
Aktivierungssperre erlauben		**SAFEv5+**
Flugmodus erlauben		**SAFEv5+**
Android Beam erlauben		**SAFEv4+**
Audioaufnahmen erlauben		**SAFEv4+**
Entwicklermodus erlauben		**SAFEv5+**
Schnellverschlüsselung erlauben		**SAFEv5+**
Firmware-Wiederherstellung erlauben		**SAFEv5+**
Auto-Sync für Google-Konten erlauben		**SAFEv5+**
S Beam erlauben		**SAFEv4+**
S Voice erlauben		**SAFEv4+**

Einstellung/Feld	Beschreibung	Mindestanforderungen
Share-List erlauben		**SAFEv4+**
Mobildatenlimit für Benutzer erlauben		**SAFEv4+**
VPN erlauben		**SAFEv2.2+**
Wallpaper-Wechsel erlauben		**SAFEv2.2+**
Wi-Fi Direct erlauben		**SAFEv4+**

Knox Premium-Beschränkungen

In dieser Konfiguration können Sie Einschränkungen für ein Samsung Knox-Gerät definieren. Diese werden auf das Gerät und nicht auf den Container angewendet.

Option	Beschreibung
Optionen für automatische Firmware-Updates erlauben	
ODE Trusted Boot-Verifizierung erlauben	
Installation einer anderen Administrator-App verhindern	Wenn diese Option aktiviert ist, wird die Installation von Apps verhindert, für die Administratorrechte erforderlich sind.
Aktivierung einer anderen Administrator-App verhindern	Wenn diese Option aktiviert ist, wird die Aktivierung von Apps verhindert, für die Administratorrechte erforderlich sind.
Common Criteria-Modus erlauben	

App Protection

In dieser Konfiguration können Sie Einstellungen für den Schutz von Apps auf Endbenutzergeräten definieren. Wenn App Protection aktiv ist, müssen Benutzer ein Kennwort definieren, sobald sie eine geschützte App zum ersten Mal starten. In der **App Protection** Konfiguration definieren Sie Kennwortanforderungen und die zu schützenden Apps. Nach einem fehlgeschlagenen Anmeldeversuch, tritt eine Anmeldeverzögerung in Kraft.

Wenn App Protection auf einem Endbenutzergerät aktiv ist, steht im Menü **Aktionen** der Ansichten **Gerät bearbeiten** und **Gerät anzeigen** die Schaltfläche **App Protection-Kennwort zurücksetzen** zur Verfügung. Außerdem kann der Benutzer das Kennwort für App Protection im Self Service Portal zurücksetzen. Weitere Informationen finden Sie im *Sophos Mobile Control Benutzerhandbuch für Android*.

Einstellung/Feld	Beschreibung
Kennworttyp	In diesem Feld definieren Sie die Mindestanforderungen für das Kennwort, das von den Benutzern festgelegt wird, zum Beispiel **6-Zeichen Kennwort**.
Gültigkeitsdauer in Minuten	Wählen Sie in diesem Feld eine Gültigkeitsdauer. Nach Ablauf der Gültigkeitsdauer können Apps nur noch durch Eingabe eines Kennworts entsperrt werden.

Klicken Sie auf die **Hinzufügen** Schaltfläche, um die Apps hinzuzufügen, die per Kennwort geschützt werden sollen. In der **Kennung bearbeiten** Ansicht stehen folgende Felder zum Konfigurieren der zu schützenden Apps zur Verfügung:

Einstellung/Feld	Beschreibung
Quelle wählen	Wählen Sie die Quelle für die Apps, die zur Liste der geschützten Apps hinzugefügt werden sollen. Je nach gewählter Quelle werden unterschiedliche Felder zum Definieren der zu schützenden Apps angezeigt: ▪ Wenn Sie **App-Liste** wählen, wird die **Apps** Dropdown-Liste mit allen für diesen Kunden verfügbaren Android-Apps angezeigt. Wählen Sie die App aus der Liste aus und klicken Sie auf **Übernehmen**. ▪ Wenn Sie **Benutzerdefiniert** auswählen, werden die Felder **Name** und **Kennung** angezeigt. Geben Sie die App-Informationen ein und klicken Sie auf **Übernehmen**.

App Control

In dieser Konfiguration können Sie Apps definieren, auf die vom Gerät nicht zugegriffen werden kann. Wird App Control verwendet, werden definierte Apps blockiert und Benutzer können sie nicht starten. Sie können beispielsweise Apps, die nicht vom Gerät entfernt werden können, blockieren.

Klicken Sie auf die **Hinzufügen** Schaltfläche, um die Apps hinzuzufügen, die blockiert werden sollen. In der **Kennung bearbeiten** Ansicht stehen folgende Felder zum Konfigurieren der zu schützenden Apps zur Verfügung:

Einstellung/Feld	Beschreibung
Quelle wählen	Wählen Sie die Quelle für die Apps, die zur Liste der geschützten Apps hinzugefügt werden sollen. Je nach gewählter Quelle werden unterschiedliche Felder zum Definieren der zu schützenden Apps angezeigt: ▪ Wenn Sie **App-Liste** wählen, wird die **Apps** Dropdown-Liste mit allen für diesen Kunden verfügbaren Android-Apps angezeigt. Wählen Sie die App aus der Liste aus und klicken Sie auf **Übernehmen**. ▪ Wenn Sie **Benutzerdefiniert** auswählen, werden die Felder **Name** und **Kennung** angezeigt. Geben Sie die App-Informationen ein und klicken Sie auf **Übernehmen**.

Exchange-ActiveSync

In dieser Konfiguration können Sie die Einstellungen für Ihren Microsoft Exchange Server definieren. Sie können mehrere **Exchange-ActiveSync** Konfigurationen hinzufügen.

Hinweis: Einige der Einstellungen in dieser Konfiguration gelten nur für Geräte mit aktivem TouchDown E-Mail Client. Diese Einstellungen sind in der Web-Konsole mit dem Label **Touchdown** gekennzeichnet.

Wenn auf einem Benutzergerät ein TouchDown Client aktiv ist, wird dieser Client ab Sophos Mobile Control 3.6 als primärer E-Mail Client verwendet.

Einstellung/Feld	Beschreibung	Mindestanforderungen
Name	Geben Sie in diesem Feld einen Konto-Namen an.	**SAFEv2+**
Server-Adresse	Geben Sie in diesem Feld die Adresse des Microsoft Exchange Servers an. **Hinweis:** Wenn Sie den SMC EAS Proxy verwenden, geben Sie die URL des SMC Proxy/Servers ein.	**SAFEv2+**
Domain	Geben Sie in diesem Feld die Domäne für das Account an.	**SAFEv2+**
Benutzer	Geben Sie in diesem Feld den Benutzer für den Account an. Sie können die Variable %_USERNAME_% verwenden. Der Server ersetzt diese durch den jeweiligen Benutzernamen, wenn für das Gerät, an das das Profil	**SAFEv2+**

Einstellung/Feld	Beschreibung	Mindestanforderungen
	gesendet wird, eine LDAP-Verbindung besteht.	
E-Mail-Adresse	Geben Sie in diesem Feld die E-Mail-Adresse für das Account an. Sie können die Variable %_EMAILADDRESS_% verwenden. Der Server ersetzt diese durch die jeweilige E-Mail-Adresse, wenn für das Gerät, an das das Profil gesendet wird, eine LDAP-Verbindung besteht.	**SAFEv2+**
Absender	Geben Sie in diesem Feld einen Absendernamen für das Konto an. Sie können die Variable %_EMAILADDRESS_% verwenden. Der Server ersetzt diese durch die jeweilige E-Mail-Adresse, wenn für das Gerät, an das das Profil gesendet wird, eine LDAP-Verbindung besteht.	**SAFEv2+**
Kennwort	Geben Sie in diesem Feld das Kennwort für das Account an.	**SAFEv2+**
Zeitraum für die Synchronisierung von E-Mails	Wählen Sie in diesem Feld den Zeitraum für die E-Mail-Synchronisierung. Dabei handelt es sich um die Anzahl an Tagen, für die E-Mails synchronisiert werden. Wenn Sie hier einen Zeitraum angeben, werden nicht alle im Posteingang enthaltenen E-Mails auf dem Mobilgerät synchronisiert, sondern nur die E-Mails aus dem angegebenen Zeitraum. Sie können folgende Optionen auswählen: ▪ **Ein Tag** ▪ **Drei Tage** ▪ **Eine Woche** ▪ **Zwei Wochen** ▪ **Ein Monat**	**SAFEv2+**
Synchronisationsintervall	Wählen Sie in diesem Feld den Abstand zwischen den einzelnen E-Mail-Synchronisierungsvorgängen: ▪ **Nie** ▪ **5 Minuten** ▪ **10 Minuten**	**SAFEv2+**

Einstellung/Feld	Beschreibung	Mindestanforderungen
	▪ **15 Minuten** ▪ **30 Minuten** ▪ **1 Stunde**	
Bei Roaming manuell synchronisieren	Wenn Sie diese Option auswählen, ist bei Roaming auf einem Gerät mit einem aktiven TouchDown E-Mail Client die manuelle Synchronisierung erforderlich.	**TouchDown**
SSL	Wählen Sie diese Option, um für die gesamte Kommunikation SSL (Secure Socket Layer) zu verwenden.	**SAFEv2+**
Standardkonto	Wählen Sie diese Option, um das Konto als das Standard-E-Mail-Konto zu definieren.	**SAFEv2+**
Erlaube alle Zertifikate	Wählen Sie diese Option, um für Übertragungsvorgänge durch den E-Mail Server alle Zertifikate zuzulassen.	**SAFEv2+**
Client-Zertifikat	Wählen Sie in diesem Feld das Client-Zertifikat für die Verbindung zu ActiveSync.	**SAFEv2+**
Copy/Paste deaktivieren	Wählen Sie diese Option, um auf Geräten mit einem aktiven TouchDown E-Mail Client die Copy/Paste-Funktion zu deaktivieren.	**TouchDown**
Kopieren ins Telefonbuch deaktivieren	Wählen Sie diese Option, um Benutzer daran zu hindern, auf Geräten mit aktivem TouchDown E-Mail Client Informationen in das Telefonbuch zu kopieren.	**TouchDown**
Drucken deaktivieren	Wählen Sie diese Option, um auf Geräten mit einem aktiven TouchDown E-Mail Client die Drucken-Funktion zu deaktivieren.	**TouchDown**
E-Mail-Weiterleitung erlauben	Wählen Sie diese Option, um die Weiterleitung von E-Mails zu erlauben.	
Verwendung des HTML-Formats erlauben	Wählen Sie diese Option, um die Verwendung des HTML-Formats in E-Mails zu erlauben.	

Einstellung/Feld	Beschreibung	Mindestanforderungen
Max. Anhangsgröße in MB	Wählen Sie die maximale E-Mail-Größe aus der Dropdown-Liste aus (**1**, **3**, **5**, **10**, **Unbegrenzt**).	**SAFEv5+**
Maximale Anzahl an Kalendertagen	Legen Sie die maximale Anzahl an Kalendertagen für die Synchronisierung von E-Mails fest.	**SAFEv5+**
Maximales E-Mail-Alter	Legen Sie das maximale Alter für die Synchronisierung von E-Mails fest.	**SAFEv5+**
Maximales E-Mail-Alter	Legen Sie das maximale Alter für die Synchronisierung von E-Mails fest.	
Inhalte	Wählen Sie aus, welcher Inhaltstyp synchronisiert werden soll. ▪ **Notizen** ▪ **Kontakte** ▪ **Kalender** ▪ **Aufgaben**	

WLAN

In dieser Konfiguration geben Sie die Einstellungen für die WLAN-Verbindungen an. Sie können mehrere **WLAN**-Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
SSID	Geben Sie in diesem Feld die ID des Drahtlosnetzwerks an.
Sicherheitstyp	In diesem Feld wählen Sie den Sicherheitstyp des WLAN aus: ▪ **Ohne** ▪ **WEP** ▪ **WPA** ▪ **EAP/PEAP** ▪ **EAP/LEAP** ▪ **EAP/TLS** ▪ **EAP/TTLS** ▪ **EAP/FAST**

Einstellung/Feld	Beschreibung
	Wenn Sie die persönlichen Einstellungen **WEP** oder **WPA** wählen, wird ein **Kennwort** Feld angezeigt. Geben Sie das relevante Kennwort ein. Wenn Sie die EAP-Einstellungen wählen, werden die Felder **Identität**, **Anonyme Identität** und **Kennwort** angezeigt. Geben Sie die erforderlichen EAP-Informationen ein. Wenn Sie die EAP-Einstellung **EAP/TTLS** wählen, wird zusätzlich das Feld **Phase 2-Autorisierung** angezeigt. Wählen Sie die Art der Autorisierung: ▪ **PAP** ▪ **CHAP** ▪ **MSCHAP** ▪ **MSCHAPv2**

VPN

Mindestanforderung: **SAFEv2+**

In dieser Konfiguration können Sie VPN-Einstellungen für Netzwerke definieren. Sie können mehrere **VPN** Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
Verbindungsname	Geben Sie in diesem Feld den Namen der Verbindung ein, der auf dem Gerät angezeigt wird.
Server	Geben Sie in diesem Feld den Host-Namen oder die IP-Adresse des Servers ein.
Verbindungstyp	Wählen Sie in diesem Feld den Verbindungstyp: ▪ **L2TP/IPsec (PSK)** Wenn Sie diesen Typ auswählen, werden die Felder **Benutzer**, **Kennwort** und **IPsec (PSK)** angezeigt. Geben Sie den Benutzer und das Kennwort ein. Geben Sie im Feld **IPsec (PSK)** den Pre-shared Key für die Authentisierung ein. ▪ **L2TP/IPsec (Zertifikat)** Wenn Sie diesen Typ auswählen, werden die Felder **Client-Zertifikat**, **Root-Zertifikat**, **Benutzer** und **Kennwort** angezeigt. Wählen Sie in den Feldern **Client-Zertifikat** und **Root-Zertifikat** die relevanten Zertifikate. Geben Sie außerdem den **Benutzer** und das zugehörige **Kennwort** ein.

Root-Zertifikat

Mindestanforderung: **SAFEv2+**

In dieser Konfiguration können Sie ein Root-Zertifikat für Geräte hochladen. Sie können mehrere **Root-Zertifikat** Konfigurationen hinzufügen. Suchen Sie im **Datei** Feld nach dem relevanten Zertifikat und klicken Sie auf **Übertragen**. Der Name des Zertifikats wird im **Zertifikatsname** Feld angezeigt.

Hinweis: Das hier hochgeladene Zertifikat ist nur für dieses Profil verfügbar. Wenn Sie Zertifikate in anderen Profilen benötigen, müssen Sie diese erneut hochladen.

Client-Zertifikat

Mindestanforderung: **SAFEv2+**

In dieser Konfiguration können Sie ein Client-Zertifikat für Geräte hochladen. Sie können mehrere **Client-Zertifikat** Konfigurationen hinzufügen. Suchen Sie im **Datei** Feld nach dem relevanten Zertifikat und klicken Sie auf **Übertragen**. Der Name des Zertifikats wird im **Zertifikatsname** Feld angezeigt. Geben Sie das **Kennwort** für das ausgewählte Zertifikat ein.

Hinweis: Das hier hochgeladene Zertifikat ist nur für dieses Profil verfügbar. Wenn Sie Zertifikate in anderen Profilen benötigen, müssen Sie diese erneut hochladen.

Antivirus

Siehe Konfigurieren von Antivirus Einstellungen für Sophos Mobile Security (Seite 126).

Webfilter

Siehe Konfigurieren von Webfilter-Einstellungen für Sophos Mobile Security (Seite 128).

Sophos Secure Workspace App

Mindestanforderung: iOS-Version **7.0+**

In dieser Konfiguration können Sie Einstellungen für die Sophos Secure Workspace App festlegen.

Hinweis:

Konfigurieren von Speicheranbietern	Einstellungen
Lokaler Speicher erlaubt es Benutzern, Dateien in Sophos Secure Workspace zu speichern und Dateien vom lokalen Speicher in den Cloud Storage hochzuladen. **Dropbox** **Egnyte**	Für jeden Storage Anbieter können Sie die folgenden Einstellungen separat definieren: **Aktivieren** Falls ausgewählt, ist der Storage Anbieter in der App sichtbar. **Offline** Falls ausgewählt, können Benutzer Dateien vom Storage Anbieter zur **Favoriten** Liste der App hinzufügen um sie offline zu lesen. **Öffnen in (verschlüsselt)**: Wenn aktiviert, können Benutzer mittels **Open In** verschlüsselte Dateien an andere Apps senden/übergeben.

Konfigurieren von Speicheranbietern	Einstellungen
Google Drive **Mediencenter** **OneDrive** **WebDAV**: **Egnyte** und **WebDAV** werden als Unternehmens-Anbieter bezeichnet. Für sie können Sie Server und Zugangsdaten zentral definieren.	**Öffnen in (Klartext)**: Wenn aktiviert, können Benutzer mittels **Open In** unverschlüsselte Dateien an andere Apps senden/übergeben. **Zwischenablage**: Wenn aktiviert, ist die Zwischenablage in der Dokumentenansicht der App aktiviert und erlaubt es Benutzern, Teile aus einem Dokument zu kopieren und sie in andere Apps einzufügen.

Einstellung/Feld	Beschreibung
Dokumente aktivieren	Aktiviert die Funktion **Dokumente**, um Unternehmensdokumente sicher zu verteilen.
App-Kennwort aktivieren	Wenn Sie diese Option aktivieren, müssen Benutzer ein zusätzliches Kennwort eingeben, um die App zu starten. Sobald die App gestartet wird nachdem die Konfiguration angewendet wurde, muss das Kennwort definiert werden.
Komplexität des Kennworts	In diesem Feld können Sie die notwendige minimale Komplexität des App-Kennworts definieren. Sicherere Kennwörter sind immer erlaubt. Kennwörter (eine Kombination von numerischen und alphanumerischen Zeichen) werden generell als sicherer angesehen als PINs (nur numerische Zeichen). Sie können folgende Einstellungen auswählen: ▪ **Beliebig**: App-Kennwörter sind keinen Einschränkungen unterworfen. ▪ **4-Ziffern PIN** ▪ **6-Ziffern PIN** ▪ **4-Zeichen Kennwort** ▪ **6-Zeichen Kennwort** ▪ **8-Zeichen Kennwort** ▪ **10-Zeichen Kennwort**
Gültigkeitsdauer in Minuten	In diesem Feld definieren Sie die Zeitspanne, während der kein App-Kennwort eingegeben werden muss sobald die App wieder im Vordergrund angezeigt wird. Wenn das Gerät gesperrt und wieder entsperrt wird, müssen die Benutzer jedenfalls das Kennwort eingeben, auch innerhalb dieser Zeitspanne. Sie können **1**, **2**, **5**, **10** oder **15** Minuten auswählen.

Einstellung/Feld	Beschreibung
Letzte Verbindung zum Server	In diesem Feld können Sie festlegen, wie lange Benutzer Sophos Secure Workspace ohne Verbindung zum Sophos Mobile Control Server verwenden können. Wenn Sophos Secure Workspace aktiviert wird und innerhalb der definierten Zeitspanne keinen Kontakt mit dem Server hatte, wird ein Sperrbildschirm mit der Schaltfläche **Wiederholen** angezeigt. Benutzer können die App nur entsperren, indem sie auf die Schaltfläche **Wiederholen** tippen, damit Sophos Secure Workspace eine Verbindung zum Server aufbaut. Kann die Verbindung aufgebaut werden, wird die App entsperrt. Falls nicht, wird der Zugriff verweigert. Sie können folgende Einstellungen definieren: ▪ **Bei jedem Zugriff**: Eine Serververbindung ist immer notwendig und die App wird gesperrt wenn der Server nicht erreichbar ist. ▪ **1 Stunde**: Eine Serververbindung ist notwendig, wenn die App eine Stunde oder später nach der letzten erfolgreichen Serververbindung aktiviert wird. ▪ **3 Stunden** ▪ **6 Stunden** ▪ **12 Stunden** ▪ **1 Tag** ▪ **3 Tage** ▪ **1 Woche** ▪ **Ohne**: Keine regelmäßige Verbindung ist notwendig.
Öffnen der App ohne Serververbindung	In diesem Feld können Sie definieren, wie oft Benutzer Sophos Secure Workspace starten können, ohne dass eine Verbindung zum Server aufgebaut wurde. **Hinweis:** Diese Einstellung setzt voraus, dass ein die Funktionalität des App-Kennworts aktiviert wurde. Es wird mitgezählt, wie oft Benutzer das Kennwort für die Sophos Secure Workspace eingeben. Wenn der Zähler die definierte Anzahl überschreitet, wird derselbe Sperrbildschirm wie für die **Letzte Verbindung zum Server** Einstellung angezeigt. Der Zähler wird zurückgesetzt, wenn eine Verbindung zum Sophos Mobile Control Server hergestellt wird. ▪ **Unbegrenzt**: Es ist keine Serververbindung notwendig. ▪ **0**: Das Starten der App ohne Serververbindung ist nicht möglich. ▪ **1**: Nach einem Start der App ist eine erfolgreiche Serververbindung notwendig. ▪ **3** ▪ **5**

Einstellung/Feld	Beschreibung
	▪ **10** ▪ **20**
Schlüsselbund aktivieren	Wenn Sie diese Option aktivieren, werden die Schlüssel in einem Schlüsselbund gespeichert. Für eine neuerliche Verwendung derselben Schlüssel müssen die Benutzer ihre Passphrase nicht erneut eingeben.
Komplexität des Kennworts	In diesem Feld können Sie die minimale Komplexität von Passphrasen definieren, die für neue Schlüssel verwendet werden sollen. Diese Schlüssel werden am Gerät erzeugt. Sicherere Passphrasen sind immer erlaubt. Sie können folgende Einstellungen auswählen: ▪ **4-Zeichen Kennwort** ▪ **6-Zeichen Kennwort** ▪ **8-Zeichen Kennwort** ▪ **10-Zeichen Kennwort**
Egnyte und **WebDAV** Für die Unternehmens-Anbieter können Sie zentral Zugangsdaten definieren. Diese können von den Benutzern nicht geändert werden. Einstellungen, die Sie nicht zentral definieren, können vom Benutzer im entsprechenden App-Dialog eingegeben werden. Beispielsweise können Sie den Server und das Benutzerkonto zentral einstellen, aber das Kennwort-Feld undefiniert lassen. Benutzer müssen dann das Kennwort eingeben, um Zugriff auf den Storage-Anbieter zu bekommen.	
Server	Geben Sie in diesem Feld Folgendes ein: ▪ Die URL zum Root-Ordner am **Unternehmensdokumente** WebDAV-Server ▪ Die URL zum Root-Ordner am **Egnyte**-Server ▪ Die URL zum Root-Ordner am **WebDAV**-Server Verwenden Sie das folgende Format: `https://server.company.com`
Benutzername	Geben Sie in diesem Feld den Benutzernamen für den entsprechenden Server ein.

Einstellung/Feld	Beschreibung
Kennwort	Geben Sie in diesem Feld das Kennwort für das entsprechende Konto an.
Zielordner	Geben Sie in diesem Feld den Zielordner für das entsprechende Konto an.

15.2 Erstellen von Container-Profilen für Android-Geräte

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Profile** und dann auf **Android**.

   Die **Profile** Ansicht wird angezeigt.

2. Klicken Sie auf **Profil anlegen** und wählen Sie **Container-Profil anlegen**.

   Die **Profil bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Version** für das neue Profil ein.
4. Geben Sie im Feld **Beschreibung** eine Beschreibung für das Profil ein.
5. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das das Profil gelten soll.
6. Klicken Sie auf die Schaltfläche **Konfiguration hinzufügen**, um Konfigurationen mit Android-Konfigurationseinstellungen zum Profil hinzuzufügen.

   Die **Verfügbare Konfigurationen** Ansicht wird angezeigt.

7. Wählen Sie die Konfiguration aus, die Sie hinzufügen möchten, und klicken Sie auf **Weiter**.

   Die Einstellungen-Ansicht der Konfiguration wird angezeigt.

8. Definieren Sie die erforderlichen Einstellungen. Eine detaillierte Liste aller verfügbaren Konfigurationen und Einstellungen finden Sie unter Verfügbare Container-Konfigurationen für Android-Geräte (Seite 61).
9. Klicken Sie auf die **Übernehmen** Schaltfläche, um Ihre Änderungen zu speichern.

   Die Konfiguration wird in der **Profil bearbeiten** Ansicht unter **Konfigurationen** angezeigt.

10. Wenn Sie alle erforderlichen Konfigurationen hinzugefügt haben, klicken Sie auf die **Speichern** Schaltfläche.

Das Profil steht für die Übertragung zur Verfügung. Es wird in der Ansicht **Profile** für **Android** angezeigt.

15.2.1 Verfügbare Container-Konfigurationen für Android-Geräte

Kennwortrichtlinien

In dieser Konfiguration können Sie Kennwortrichtlinien für Geräte definieren. Sie können nur eine **Kennwortrichtlinien** Konfiguration in einem Profil hinzufügen.

Wenn Sie die **Kennwortrichtlinien** Konfiguration auswählen, wird das **Kennworttyp** Feld angezeigt. Wählen Sie in diesem Feld die Art des Kennworts, dass Sie definieren möchten:

- **Beliebig**

Wenn Sie diese Einstellung wählen, müssen Benutzer ein Kennwort auf dem Endgerät einstellen. Für das Kennwort gelten jedoch keine Anforderungen oder Einschränkungen. Wenn Sie diese Option wählen, sind für die **Kennwortrichtlinien** Konfiguration keine weiteren Einstellungen erforderlich.

- **Alphabetisch**
- **PIN**
- **Alphanumerisch**
- **Komplex**

Wenn Sie **Alphabetisch**, **PIN** oder **Alphanumerisch** auswählen, werden die folgenden Felder angezeigt:

Einstellung/Feld	Beschreibung
Minimale Länge des Kennworts	Gibt an, wie viele Zeichen ein Kennwort mindestens enthalten muss.
Inaktivitätszeit in Sekunden bis zur Abfrage des Kennworts	In diesem Feld können Sie festlegen, wann (in Sekunden) das Gerät nach Nichtbenutzung gesperrt werden soll. Das Gerät lässt sich durch Eingabe des Kennworts entsperren.
Gültigkeitsdauer des Kennworts (Tage)	Fordert eine Änderung des Kennworts im angegebenen Intervall (in Tagen).
Maximale Anzahl fehlerhafter Loginversuche, bis das Gerät zurückgesetzt wird	In diesem Feld können Sie die Höchstanzahl an fehlgeschlagenen Eingabeversuchen für das Kennwort eingeben. Nach Erreichen der Höchstanzahl wird das Gerät zurückgesetzt.
Anzahl der letzten Kennwörter, die nicht benutzt werden dürfen	In diesem Feld können Sie festlegen, wie viele alte Kennwörter gespeichert und mit neu definierten Kennwörtern verglichen werden. Wenn ein Benutzer ein neues Kennwort festlegt, wird es nicht akzeptiert, wenn es mit einem bereits benutzten Kennwort übereinstimmt. Wertebereich: 1 bis 5 oder kein Wert.

Wenn Sie **Komplex** auswählen, werden zusätzlich zu den für die anderen Kennworttypen angezeigten Felder die folgenden Felder angezeigt:

Einstellung/Feld	Beschreibung
Minimale Anzahl an Buchstaben	Gibt an, wie viele Buchstaben ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Kleinbuchstaben	Gibt an, wie viele Kleinbuchstaben ein Kennwort mindestens enthalten muss.

Einstellung/Feld	Beschreibung
Minimale Anzahl von Großbuchstaben	Gibt an, wie viele Großbuchstaben ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Zeichen, die kein Buchstabe sind	Gibt an, wie viele nicht-alphabetische Zeichen (zum Beispiel & oder !) ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Zahlen	Gibt an, wie viele Zahlen ein Kennwort mindestens enthalten muss.
Minimale Anzahl von Sonderzeichen	Gibt an, wie viele Sonderzeichen (zum Beispiel !"§$%&/()=,.-;:_@<>) ein Kennwort mindestens enthalten muss.

Einschränkungen

In dieser Konfiguration können Sie Einschränkungen für Geräte definieren. Sie können nur eine **Einschränkungen** Konfiguration in einem Profil hinzufügen.

Einstellung/Feld	Mindestanforderungen
Bildschirmaufnahme erlauben	**KNOXv2+**
Kamera erlauben	**KNOXv2+**
Zwischenablage erlauben	**KNOXv2+**
Share-List erlauben	**KNOXv2+**
Mikrofon erlauben	**KNOXv2+**
Verwendung der sicheren Tastatur durchsetzen	**KNOXv2+**
Hinzufügen neuer E-Mail-Konten erlauben	**KNOXv2+**
Sie können den Container so konfigurieren, dass die manuelle Installation von Apps beschränkt wird. Sie können **Erlaubte Apps** und **Nicht erlaubte Apps** hinzufügen. Wählen Sie entweder **Erlaubte hinzufügen** oder **Nicht erlaubte Apps** und klicken Sie auf **Hinzufügen**. Wählen Sie im Dialog **App bearbeiten** die App aus der Dropdown-Liste aus oder klicken Sie auf **Benutzerdefiniert** und geben Sie **App-Name** und **Kennung** ein. Klicken Sie auf **Hinzufügen**. Vom Server initiierte Installationen werden automatisch zugelassen.	

Exchange-ActiveSync

In dieser Konfiguration können Sie die Einstellungen für Ihren Microsoft Exchange Server definieren. Sie können mehrere **Exchange-ActiveSync** Konfigurationen hinzufügen.

Hinweis: Einige der Einstellungen in dieser Konfiguration gelten nur für Geräte mit aktivem TouchDown E-Mail Client. Diese Einstellungen sind in der Web-Konsole mit dem Label **Touchdown** gekennzeichnet.

Wenn auf einem Benutzergerät ein TouchDown Client aktiv ist, wird dieser Client ab Sophos Mobile Control 3.6 als primärer E-Mail Client verwendet.

Einstellung/Feld	Beschreibung	Mindestanforderungen
Name	Geben Sie in diesem Feld einen Konto-Namen an.	**SAFEv2+**
Server-Adresse	Geben Sie in diesem Feld die Adresse des Microsoft Exchange Servers an. **Hinweis:** Wenn Sie den SMC EAS Proxy verwenden, geben Sie die URL des SMC Proxy/Servers ein.	**SAFEv2+**
Domäne	Geben Sie in diesem Feld die Domäne für das Account an.	**SAFEv2+**
Benutzer	Geben Sie in diesem Feld den Benutzer für den Account an. Sie können die Variable %_USERNAME_% verwenden. Der Server ersetzt diese durch den jeweiligen Benutzernamen, wenn für das Gerät, an das das Profil gesendet wird, eine LDAP-Verbindung besteht.	**SAFEv2+**
E-Mail-Adresse	Geben Sie in diesem Feld die E-Mail-Adresse für das Account an. Sie können die Variable %_EMAILADDRESS_% verwenden. Der Server ersetzt diese durch die jeweilige E-Mail-Adresse, wenn für das Gerät, an das das Profil gesendet wird, eine LDAP-Verbindung besteht.	**SAFEv2+**
Absender	Geben Sie in diesem Feld einen Absendernamen für das Konto an. Sie können die Variable %_EMAILADDRESS_% verwenden. Der Server ersetzt diese durch die jeweilige E-Mail-Adresse, wenn für das Gerät, an das das Profil gesendet wird, eine LDAP-Verbindung besteht.	**SAFEv2+**

Einstellung/Feld	Beschreibung	Mindestanforderungen
Kennwort	Geben Sie in diesem Feld das Kennwort für das Account an.	**SAFEv2+**
Zeitraum für die Synchronisierung von E-Mails	Wählen Sie in diesem Feld den Zeitraum für die E-Mail-Synchronisierung. Dabei handelt es sich um die Anzahl an Tagen, für die E-Mails synchronisiert werden. Wenn Sie hier einen Zeitraum angeben, werden nicht alle im Posteingang enthaltenen E-Mails auf dem Mobilgerät synchronisiert, sondern nur die E-Mails aus dem angegebenen Zeitraum. Sie können folgende Optionen auswählen: ▪ **Ein Tag** ▪ **Drei Tage** ▪ **Eine Woche** ▪ **Zwei Wochen** ▪ **Ein Monat**	**SAFEv2+**
Synchronisationsintervall	Wählen Sie in diesem Feld den Abstand zwischen den einzelnen E-Mail-Synchronisierungsvorgängen: ▪ **Nie** ▪ **5 Minuten** ▪ **10 Minuten** ▪ **15 Minuten** ▪ **30 Minuten** ▪ **1 Stunde**	**SAFEv2+**
SSL	Wählen Sie diese Option, um für die gesamte Kommunikation SSL (Secure Socket Layer) zu verwenden.	**SAFEv2+**
Standardkonto	Wählen Sie diese Option, um das Konto als das Standard-E-Mail-Konto zu definieren.	**SAFEv2+**
Erlaube alle Zertifikate	Wählen Sie diese Option, um für Übertragungsvorgänge durch den E-Mail Server alle Zertifikate zuzulassen.	**SAFEv2+**
E-Mail-Weiterleitung erlauben	Wählen Sie diese Option, um die Weiterleitung von E-Mails zu erlauben.	

Einstellung/Feld	Beschreibung	Mindestanforderungen
Verwendung des HTML-Formats erlauben	Wählen Sie diese Option, um die Verwendung des HTML-Formats in E-Mails zu erlauben.	
Max. Anhangsgröße in MB	Wählen Sie die maximale E-Mail-Größe aus der Dropdown-Liste aus (**1**, **3**, **5**, **10**, **Unbegrenzt**).	**SAFEv5+**
Maximale Anzahl an Kalendertagen	Legen Sie die maximale Anzahl an Kalendertagen für die Synchronisierung von E-Mails fest.	**SAFEv5+**
Maximales E-Mail-Alter	Legen Sie das maximale Alter für die Synchronisierung von E-Mails fest.	**SAFEv5+**
Maximales E-Mail-Alter	Legen Sie das maximale Alter für die Synchronisierung von E-Mails fest.	
Inhalte	Wählen Sie aus, welcher Inhaltstyp synchronisiert werden soll. ▪ **Notizen** ▪ **Kontakte** ▪ **Kalender** ▪ **Aufgaben**	

15.3 Erstellen von Profilen für iOS-Geräte

Für das Erstellen von Profilen für iOS-Geräte bietet Sophos Mobile Control zwei Verfahren:

- Sie können iOS-Profile direkt in der Web-Konsole anlegen.
- Sie können mit der Apple iPhone Configuration Utility erstellte Profile in die Web-Konsole importieren.

15.3.1 Erstellen von iOS-Profilen in der Web-Konsole

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Profile** und dann auf **Apple iOS**.

   Die **Profile** Ansicht wird angezeigt.

2. Klicken Sie auf **Profil anlegen** und wählen Sie **Profil anlegen**.

   Die **Profil bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen**, Ihre **Organisation** (das Feld wird automatisch mit Ihrem Kundennamen ausgefüllt) und eine **Beschreibung** ein. Die Angabe zur **Version** ist optional.

4. Legen Sie im **Durch Benutzer entfernbar** Feld fest, ob Benutzer das Profil von ihrem Gerät entfernen dürfen:
   - **Immer**
   - **Mit Authentifizierung**

     Wenn Sie diese Option auswählen, wird unter dem **Durch Benutzer entfernbar** Feld das Feld **Kennwort für Authentisierung** angezeigt. Geben Sie das für das Entfernen des Profils erforderliche Kennwort ein. Um Benutzern zu ermöglichen, das Profil zu entfernen, teilen Sie ihnen das Kennwort mit.

   - **Nie**
5. Im Feld **Automatisch entfernen am** können Sie ein Datum angeben, an dem das Profil automatisch von Endbenutzergeräten entfernt wird. Das Profil wird am festgelegten Datum um 23:00 entfernt.
6. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das das Profil gelten soll.

   Hinweis: Das **Betriebssysteme** Feld zeigt alle iOS-Versionen, die derzeit im System verfügbar sind. Für die einzelnen iOS-Versionen werden u. U. nicht alle Konfigurationseinstellungen unterstützt. Wenn Sie unter **Betriebssysteme** alle Versionen auswählen, haben je nach iOS-Version auf dem Endbenutzergerät einige Einstellungen unter Umständen keine Auswirkung.
7. Klicken Sie auf **Konfiguration hinzufügen**.

   Die **Verfügbare Konfigurationen** Ansicht wird angezeigt.
8. Wählen Sie die Konfiguration aus, die Sie hinzufügen möchten, und klicken Sie auf **Weiter**.

   Die Einstellungen-Ansicht der Konfiguration wird angezeigt.
9. Definieren Sie die erforderlichen Einstellungen. Für eine detaillierte Liste aller verfügbaren Konfigurationen und Einstellungen siehe Verfügbare iOS-Konfigurationen (Seite 67).
10. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

    Die Konfiguration wird in der **Profil bearbeiten** Ansicht unter **Konfigurationen** angezeigt.
11. Fügen Sie nach Wunsch weitere Konfigurationen hinzu.
12. Wenn Sie alle erforderlichen Konfigurationen hinzugefügt haben, klicken Sie auf die Schaltfläche **Speichern**.

Das Profil steht für die Übertragung zur Verfügung. Es wird in der **Profile** Ansicht angezeigt.

15.3.2 Verfügbare iOS-Konfigurationen

Die folgenden Konfigurationen sind für iOS-Profile in der **Verfügbare Konfigurationen** Ansicht verfügbar, wenn Sie ein Profil erstellen oder bearbeiten. Einige Konfigurationen lassen sich in einem Profil nur einmal hinzufügen, andere mehrmals.

Hinweis: Die unterstützten Einstellungen hängen von der iOS-Version ab, die auf den einzelnen Geräten in Gebrauch ist. Je nach Endbenutzergerät haben einige Einstellungen unter Umständen keine Auswirkung. In der Web-Konsole wird jeweils angegeben, wenn eine Einstellung nur ab einer bestimmten iOS-Version oder nur im **supervised** Modus unterstützt wird. In den folgenden Beschreibungen finden Sie diese Informationen jeweils zu Beginn der einzelnen Abschnitte oder in einer Tabellenspalte zu den etwaigen Mindestanforderungen.

Kennwortrichtlinien

In dieser Konfiguration können Sie Kennwortrichtlinien für Geräte definieren. Sie können nur eine **Kennwortrichtlinien** Konfiguration in einem Profil hinzufügen.

Einstellung/Feld	Beschreibung
Einfache Werte erlauben	Wenn Sie diese Option auswählen, dürfen Benutzer aufeinander folgende oder wiederholte Zeichen in ihrem Kennwort verwenden, zum Beispiel "1111" oder "abcde".
Alphanumerische Werte erforderlich	Wenn Sie diese Option auswählen, müssen Kennwörter mindestens einen Buchstaben oder eine Zahl enthalten.
Minimale Länge des Kennworts	Gibt an, wie viele Zeichen ein Kennwort mindestens enthalten muss.
Mindestanzahl von komplexen Zeichen	Gibt an, wie viele nicht-alphanumerische Zeichen (zum Beispiel & oder !) ein Kennwort mindestens enthalten muss.
Maximale Kennwortgültigkeit (1 - 730 Tage oder ohne)	Fordert eine Änderung des Kennworts im angegebenen Intervall. Wertebereich: 0 (keine Kennwortänderung erforderlich) bis 730 Tage.
Automatische Sperre (Minuten)	In diesem Feld können Sie den Höchstwert festlegen, den der Benutzer auf dem Gerät konfigurieren darf. Mit der automatischen Sperre wird festgelegt, wann (in Minuten) das Gerät nach Nichtbenutzung gesperrt werden soll.
Anzahl der letzten Kennwörter, die nicht benutzt werden dürfen (1 - 50 oder 0)	In diesem Feld können Sie festlegen, wie viele alte Kennwörter gespeichert und mit neu definierten Kennwörtern verglichen werden. Wenn ein Benutzer ein neues Kennwort festlegt, wird es nicht akzeptiert, wenn es mit einem bereits benutzten Kennwort übereinstimmt. Wertebereich: 1 bis 50 oder 0 (keine Kennworthistorie).
Zeitgrenze für Gerätesperrung	In diesem Feld können Sie den Höchstwert festlegen, den der Benutzer auf dem Gerät konfigurieren darf. Mit der Zeitgrenze für die Gerätesperrung können Sie festlegen, wie lang ein Gerät nach einer Sperre ohne Kennwort-Eingabeaufforderung entsperrt werden darf. Wenn Sie **Ohne** auswählen, kann der Benutzer einen beliebigen verfügbaren Zeitraum wählen. Wenn Sie **Sofort** auswählen, müssen

Einstellung/Feld	Beschreibung
	Benutzer immer, wenn sie ihre Geräte entsperren, ein Kennwort eingeben.
Maximale Anzahl fehlerhafter Loginversuche, bis das Gerät zurückgesetzt wird	In diesem Feld können Sie die Höchstanzahl an fehlgeschlagenen Eingabeversuchen für das Kennwort eingeben. Nach Erreichen der Höchstanzahl wird das Gerät zurückgesetzt. Nach sechs fehlgeschlagenen Versuchen wird eine Zeitverzögerung verhängt. Ein erneuter Versuch kann erst nach Ablauf der Verzögerung unternommen werden. Diese Verzögerung wird mit jedem fehlgeschlagenen Versuch größer. Nach dem letzten fehlgeschlagenen Versuch werden alle Daten und Einstellungen sicher vom Gerät entfernt. Die Zeitverzögerung startet nach dem sechsten Versuch. Wenn Sie also diesen Wert auf **6** oder einen niedrigeren Wert setzen, wird keine Verzögerung ausgelöst. In diesem Fall wird das Gerät zurückgesetzt, sobald die maximale Anzahl an Fehlversuchen überschritten ist.

Einschränkungen

In dieser Konfiguration können Sie Einschränkungen für Geräte definieren. Sie können nur eine **Einschränkungen** Konfiguration in einem Profil hinzufügen.

Einstellung/Feld	Beschreibung	Mindestanforderungen
Gerät		
Installation von Programmen erlauben	Wenn Sie diese Option deaktivieren, wird der App Store deaktiviert und sein Symbol wird vom Home-Bildschirm entfernt. Benutzer können keine Apps über den App Store oder iTunes installieren oder aktualisieren.	
Verwendung der Kamera erlauben	Wenn Sie diese Option deaktivieren, werden Kameras vollständig deaktiviert. Das Kamera-Symbol wird vom Home-Bildschirm entfernt. Benutzer können weder Fotos machen, Videos aufzeichnen noch FaceTime benutzen.	
FaceTime erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine FaceTime Anrufe tätigen oder erhalten.	

Einstellung/Feld	Beschreibung	Mindestanforderungen
Screenshot erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Screenshots vom Display erstellen.	✖
Automatische Synchronisierung beim Roaming erlauben	Wenn Sie diese Option deaktivieren, synchronisieren sich Geräte beim Roaming nur dann, wenn der Benutzer auf ein Konto zugreift.	✖
Siri erlauben	Wenn Sie diese Option deaktivieren, können Benutzer Siri, Sprachbefehle oder die Diktierfunktion nicht verwenden.	**5.0+**
Siri erlauben während das Gerät gesperrt ist	Wenn Sie diese Option deaktivieren, müssen Benutzer ihre Geräte durch Eingabe ihres Kennworts entsperren, damit Sie Siri benutzen können.	**6.0+**
Websuche für Siri erlauben	Wenn Sie diese Option deaktivieren, führt Siri keine Websuche durch.	**7.0+**, **supervised**
Filtern von vulgären Ausdrücken für Siri erzwingen	Wenn Sie diese Option deaktivieren, wird das Filtern von vulgären Ausdrücken für Siri nicht durchgesetzt.	**6.0+**, **supervised**
Sprachwahl erlauben	Wenn Sie diese Option deaktivieren, können Benutzer nicht mit Sprachwahl auf ihrem Telefon wählen.	✖
Passbook bei Gerätesperre erlauben	Wenn Sie diese Option deaktivieren, zeigt das Gerät keine Passbook-Benachrichtigungen, wenn es gesperrt ist.	**6.0+**
App-interne Käufe erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine App-internen Käufe durchführen.	✖
Benutzer muss für alle Einkäufe das iTunes Store-Kennwort eingeben	Wenn Sie diese Option auswählen, müssen Benutzer für jeden Einkauf ihr Apple ID Kennwort eingeben. In der Regel gilt nach einem Einkauf eine kurze Wartezeit, bevor sich Benutzer für weitere Einkäufe erneut anmelden müssen.	**5.0+**
Mehrspielermodus erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Spiele im Mehrspielermodus im Game Center spielen.	✖

Einstellung/Feld	Beschreibung	Mindestanforderungen
Game Center erlauben	Wenn Sie diese Option deaktivieren, kann Game Center nicht auf dem Gerät benutzt werden.	**6.0+**, **supervised**
Hinzufügen von Game Center-Freunden zulassen	Wenn Sie diese Option deaktivieren, können Benutzer keine Freunde im Game Center hinzufügen.	
Änderung der "Freunde suchen"-Einstellungen erlauben	Wenn Sie diese Option deaktivieren, sind Änderungen an der App "Freunde suchen" deaktiviert.	**7.0+**, **supervised**
Datenaustausch per Kabel erlauben	Wenn Sie diese Option auswählen, ist der Datenaustausch per Kabel mit Ausnahme des Supervision Host deaktiviert. Wenn kein Supervision Host Zertifikat konfiguriert wurde, wird jeglicher Austausch deaktiviert.	**7.0+**, **supervised**
AirDrop erlauben	Wenn Sie diese Option deaktivieren, ist das Teilen von Inhalten mit AirDrop auf dem Gerät nicht zulässig.	**7.0+**, **supervised**
Zugriff auf das Kontrollzentrum im Sperrbildschirm erlauben	Wenn Sie diese Option deaktivieren, lassen sich Einstellungen nicht mit dem Kontrollzentrum verwalten, wenn der Gerätebildschirm gesperrt ist.	**7.0+**
Zugriff auf die Mitteilungszentrale im Sperrbildschirm erlauben	Wenn Sie diese Option deaktivieren, ist die Mitteilungszentrale nicht verfügbar, wenn der Gerätebildschirm gesperrt ist.	**7.0+**
Zugriff auf die Heute-Ansicht im Sperrbildschirm erlauben	Wenn Sie diese Option deaktivieren, ist die Heute-Ansicht nicht verfügbar, wenn der Gerätebildschirm gesperrt ist.	**7.0+**
Over-the-air PKI Updates erlauben	Wenn Sie diese Option deaktivieren, sind Over-the-air PKU-Updates nicht möglich.	**7.0+**
Einkauf von Büchern in iBooks erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Bücher in iBooks erwerben.	**6.0+**, **supervised**
Einkauf von erotischen Büchern in iBooks erlauben	Wenn Sie diese Option deaktivieren, sind erotische Bücher in iBooks nicht verfügbar.	**6.0+**, **supervised**
Installation von Konfigurationsprofilen durch den Benutzer erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Konfigurationsprofile installieren.	**6.0+**, **supervised**

Einstellung/Feld	Beschreibung	Mindestanforderungen
iMessage erlauben	Wenn Sie diese Option deaktivieren, können Benutzer iMessage nicht zum Verfassen von Nachrichten verwenden.	**6.0+**, **supervised**
Deinstallation von Apps erlauben	Wenn Sie diese Option deaktivieren, können Benutzer keine Apps von ihren Geräten entfernen.	**6.0+**, **supervised**
Löschen aller Inhalte und Einstellungen erlauben		**8.0+**, **supervised**
Internetsuchergebnis für Spotlight erlauben		**8.0+**, **supervised**
Aktivierung der Beschränkungsoption erlauben		**8.0+**, **supervised**
Handoff erlauben		**8.0+**
Unternehmensdaten		
Öffnen von Dokumenten nur innerhalb von managed Apps/Konten erlauben	Mit dieser Einstellungen können Sie eine Einschränkung für das Öffnen von Dokumenten mit Apps/Accounts (zum Beispiel einem Firmen-E-Mail-Account), die von Sophos Mobile Control verwaltet werden, definieren. Zum Beispiel: Wenn diese Option ausgewählt ist und Benutzer über ein von Sophos Mobile Control verwaltetes E-Mail-Account und von Sophos Mobile Control verwaltete Apps auf Ihren Geräten verfügen, können die Anhänge aus dem verwalteten E-Mail-Account nur mit verwalteten Apps geöffnet werden. Auf diese Weise können Sie verhindern, dass Unternehmensdokumente mit unmanaged Apps geöffnet werden.	**7.0+**
Öffnen von Dokumenten nur innerhalb von unmanaged Apps/Konten erlauben	Mit dieser Einstellungen können Sie eine Einschränkung für das Öffnen von Dokumenten mit Apps/Accounts (zum Beispiel einem privaten E-Mail-Account), die nicht von Sophos Mobile Control verwaltet werden, definieren. Zum Beispiel: Wenn diese Option ausgewählt ist und Benutzer über einen nicht durch Sophos Mobile Control verwalteten E-Mail-Account und nicht Sophos Mobile Control verwaltete Apps auf Ihren Geräten verfügen, können die Anhänge aus dem nicht verwalteten E-Mail-Account	**7.0+**

Einstellung/Feld	Beschreibung	Mindestanforderungen
	nur mit nicht verwalteten Apps geöffnet werden. Auf diese Weise können Sie verhindern, dass persönliche Dokumente mit managed Apps geöffnet werden.	
Managed Apps mit Cloud-Sync erlauben		**8.0+**
Backup für Enterprise Books erlauben		**8.0+**
Enterprise Books Notes und Highlights-Sync erlauben		**8.0+**
Programme		
Verwendung von YouTube erlauben	Wenn Sie diese Option deaktivieren, wird YouTube deaktiviert. Das YouTube-Symbol wird vom Home-Bildschirm entfernt. **Hinweis:** Diese Einstellung gilt nur für iOS-Versionen vor Version 6.	**4.0-5.0**
iTunes Store darf verwendet werden	Wenn Sie diese Option deaktivieren, wird der iTunes Store deaktiviert und sein Symbol wird vom Home-Bildschirm entfernt. Benutzer können Inhalte weder in der Vorschau ansehen, noch kaufen oder herunterladen.	✖
Verwendung von Safari erlauben	Wenn Sie diese Option deaktivieren, wird der Safari Web Browser deaktiviert und sein Symbol wird vom Home-Bildschirm entfernt. Dies verhindert auch, dass Benutzer Webclips öffnen.	✖
Automatisches Ausfüllen aktivieren	Wenn Sie diese Option deaktivieren, werden Benutzereingaben in Webformularen von Safari nicht wiedererkannt.	**5.0+**
Betrugswarnung erzwingen	Wenn Sie diese Option auswählen, verhindert Safari, dass Benutzer als betrügerisch oder schädlich erkannte Websites aufrufen.	**5.0+**
JavaScript aktivieren	Wenn Sie diese Option deaktivieren, ignoriert Safari JavaScript auf Websites.	**6.0-6.1**
Pop-Ups unterdrücken	Wenn Sie diese Option auswählen, unterdrückt Safari Popups.	**5.0+**

Einstellung/Feld	Beschreibung	Mindestanforderungen
Cookies akzeptieren	In diesem Feld können Sie festlegen, ob Cookies akzeptiert werden sollen: ▪ Immer ▪ Nie ▪ Von besuchten Webseiten	**5.0+**
Änderung der Einstellungen für mobile Datenverbindungen pro App erlauben	Wenn Sie diese Option deaktivieren, können Benutzer die Einstellungen für die mobile Datenverbindung pro App nicht ändern.	**7.0+**, **supervised**
iCloud		
Backup erlauben	Wenn Sie diese Option auswählen, können Benutzer ihre Geräte im iCloud-Speicher sichern.	**5.0+**
Dokumentsynchronisierung erlauben	Wenn Sie diese Option auswählen, können Benutzer ihre Dokumente im iCloud-Speicher sichern.	**5.0+**
Fotostream zulassen	Wenn Sie diese Option auswählen, können Benutzer Fotostreaming aktivieren. **Hinweis:** Wenn Sie ein Konfigurationsprofil installieren, dass die Benutzung von Fotostream einschränkt, werden Fotostream-Fotos vom Gerät des Benutzers entfernt. Es ist außerdem nicht möglich, Fotos aus dem Fotoordner an Fotostream zu senden. Wenn keine anderen Kopien dieser Fotos existieren, gehen diese u. U. verloren.	**5.0+**
Freigegebene Fotostreams erlauben	Wenn Sie diese Option auswählen, können Benutzer andere einladen, ihre Fotostreams anzusehen. Außerdem können in diesem Fall Benutzer die freigegebenen Fotostreams anderer ansehen.	**6.0+**
Schlüsselbundsynchronisierung erlauben	Wenn Sie diese Option deaktivieren, ist die iCloud-Funktion für die Synchronisierung von Kennwörtern über verschiedene iOS- und OS X-Geräte hinweg nicht auf dem Gerät erlaubt.	**7.0+**
Sicherheit und Privatsphäre		

Einstellung/Feld	Beschreibung	Mindestanforderungen
Senden von Diagnosedaten an Apple erlauben	Wenn Sie diese Option deaktivieren, werden keine iOS-Diagnosedaten an Apple gesendet.	**5.0+**
Annehmen nicht vertrauenswürdiger TLS-Zertifikate durch Benutzer	Wenn Sie diese Option deaktivieren, werden Benutzer nicht gefragt, ob sie einem Zertifikat vertrauen möchten, das nicht verifiziert werden kann. Diese Einstellung gilt für Safari und Mail-Kontakte und Kalender-Accounts.	**5.0+**
Kontoänderungen erlauben	Wenn Sie diese Option deaktivieren, sind Kontoänderungen deaktiviert. Auf dem Gerät ist das **Konto** Menü nicht verfügbar.	**7.0+**, **supervised**
Touch ID zm Entsperren des Geräts erlauben	Wenn Sie diese Option deaktivieren, kann das Gerät nicht per Touch ID entsperrt werden.	**7.0+**
Limitierung von Ad-Tracking erzwingen	Wenn Sie diese Option auswählen, werden anonyme Benutzerdaten, die Apps für die Adressierung von Werbung benutzen, nicht mehr bereit gestellt.	**7.0+**, **supervised**
Verschlüsselte Backups erzwingen	Wenn Sie diese Option auswählen, müssen Benutzer Backups in iTunes verschlüsseln.	**7.0+**, **supervised**
Inhaltsbewertung		
Anstößige Musik und Podcasts erlauben	Wenn Sie diese Option deaktivieren, werden anstößiger Musik- oder Video-Inhalte im iTunes Store nicht angezeigt. Anstößige Inhalte werden von den jeweiligen Anbietern, zum Beispiel Plattenfirmen, bei der Auflistung im iTunes Store entsprechend gekennzeichnet.	❌

Roaming-/Hotspot-Einstellungen

Mindestanforderung: iOS-Version **7.0+**

In dieser Konfiguration können Sie die Einstellungen für Roaming und persönliche Hotspots definieren.

Hinweis: Benutzer können diese Einstellungen auf ihren Geräten jederzeit ändern.

Einstellung/Feld	Beschreibung
Sprachroaming aktivieren	Wenn Sie diese Option deaktivieren, wird Sprachroaming auf dem Gerät deaktiviert.
Datenroaming aktivieren	Wenn Sie diese Option deaktivieren, wird Datenroaming auf dem Gerät deaktiviert.
Persönlichen Hotspot aktivieren	Wenn Sie diese Einstellung deaktiveren, kann das Gerät nicht als persönlicher Hotspot konfiguriert werden.

Sophos Secure Workspace App

Mindestanforderung: iOS-Version **7.0+**

In dieser Konfiguration können Sie Einstellungen für die Sophos Secure Workspace App festlegen.

Hinweis:

Konfigurieren von Speicheranbietern	Einstellungen
Lokaler Speicher erlaubt es Benutzern, Dateien in Sophos Secure Workspace zu speichern und Dateien vom lokalen Speicher in den Cloud Storage hochzuladen. **Dropbox** **Egnyte** **Google Drive** **Mediencenter** **OneDrive** **WebDAV**: **Egnyte** und **WebDAV** werden als Unternehmens-Anbieter bezeichnet. Für sie können Sie Server und Zugangsdaten zentral definieren.	Für jeden Storage Anbieter können Sie die folgenden Einstellungen separat definieren: **Aktivieren** Falls ausgewählt, ist der Storage Anbieter in der App sichtbar. **Offline** Falls ausgewählt, können Benutzer Dateien vom Storage Anbieter zur **Favoriten** Liste der App hinzufügen um sie offline zu lesen. **Öffnen in (verschlüsselt)**: Wenn aktiviert, können Benutzer mittels **Open In** verschlüsselte Dateien an andere Apps senden/übergeben. **Öffnen in (Klartext)**: Wenn aktiviert, können Benutzer mittels **Open In** unverschlüsselte Dateien an andere Apps senden/übergeben. **Zwischenablage**: Wenn aktiviert, ist die Zwischenablage in der Dokumentenansicht der App aktiviert und erlaubt es Benutzern, Teile aus einem Dokument zu kopieren und sie in andere Apps einzufügen.

Einstellung/Feld	Beschreibung
Dokumente aktivieren	Aktiviert die Funktion **Dokumente**, um Unternehmensdokumente sicher zu verteilen.

Einstellung/Feld	Beschreibung
App-Kennwort aktivieren	Wenn Sie diese Option aktivieren, müssen Benutzer ein zusätzliches Kennwort eingeben, um die App zu starten. Sobald die App gestartet wird nachdem die Konfiguration angewendet wurde, muss das Kennwort definiert werden.
Kennworttyp	In diesem Feld können Sie die notwendige minimale Komplexität des App-Kennworts definieren. Sicherere Kennwörter sind immer erlaubt. Kennwörter (eine Kombination von numerischen und alphanumerischen Zeichen) werden generell als sicherer angesehen als PINs (nur numerische Zeichen). Sie können folgende Einstellungen auswählen: ▪ **Beliebig**: App-Kennwörter sind keinen Einschränkungen unterworfen. ▪ **4-Ziffern PIN** ▪ **6-Ziffern PIN** ▪ **4-Zeichen Kennwort** ▪ **6-Zeichen Kennwort** ▪ **8-Zeichen Kennwort** ▪ **10-Zeichen Kennwort**
Gültigkeitsdauer in Minuten	In diesem Feld definieren Sie die Zeitspanne, während der kein App-Kennwort eingegeben werden muss sobald die App wieder im Vordergrund angezeigt wird. Wenn das Gerät gesperrt und wieder entsperrt wird, müssen die Benutzer jedenfalls das Kennwort eingeben, auch innerhalb dieser Zeitspanne. Sie können **1**, **2**, **5**, **10** oder **15** Minuten auswählen.
Letzte Verbindung zum Server	In diesem Feld können Sie festlegen, wie lange Benutzer Sophos Secure Workspace ohne Verbindung zum Sophos Mobile Control Server verwenden können. Wenn Sophos Secure Workspace aktiviert wird und innerhalb der definierten Zeitspanne keinen Kontakt mit dem Server hatte, wird ein Sperrbildschirm mit der Schaltfläche **Wiederholen** angezeigt. Benutzer können die App nur entsperren, indem sie auf die Schaltfläche **Wiederholen** tippen, damit Sophos Secure Workspace eine Verbindung zum Server aufbaut. Kann die Verbindung aufgebaut werden, wird die App entsperrt. Falls nicht, wird der Zugriff verweigert. Sie können folgende Einstellungen definieren: ▪ **Bei jedem Zugriff**: Eine Serververbindung ist immer notwendig und die App wird gesperrt wenn der Server nicht erreichbar ist. ▪ **1 Stunde**: Eine Serververbindung ist notwendig, wenn die App eine Stunde oder später nach der letzten erfolgreichen Serververbindung aktiviert wird.

Einstellung/Feld	Beschreibung
	▪ **3 Stunde** ▪ **6 Stunde** ▪ **12 Stunde** ▪ **1 Tag** ▪ **3 Tage** ▪ **1 Woche** ▪ **Ohne**: Keine regelmäßige Verbindung ist notwendig.
Öffnen der App ohne Serververbindung	In diesem Feld können Sie definieren, wie oft Benutzer Sophos Mobile Encryption starten können, ohne dass eine Verbindung zum Server aufgebaut wurde. **Hinweis:** Diese Einstellung setzt voraus, dass ein die Funktionalität des App-Kennworts aktiviert wurde. Es wird mitgezählt, wie oft Benutzer das Kennwort für die Sophos Secure Workspace eingeben. Wenn der Zähler die definierte Anzahl überschreitet, wird derselbe Sperrbildschirm wie für die **Letzte Verbindung zum Server** Einstellung angezeigt. Der Zähler wird zurückgesetzt, wenn eine Verbindung zum Sophos Mobile Control Server hergestellt wird. ▪ **Unbegrenzt**: Es ist keine Serververbindung notwendig. ▪ **0**: Das Starten der App ohne Serververbindung ist nicht möglich. ▪ **1**: Nach einem Start der App ist eine erfolgreiche Serververbindung notwendig. ▪ **3** ▪ **5** ▪ **10** ▪ **20**
Schlüsselbund aktivieren	Wenn Sie diese Option aktivieren, werden die Schlüssel in einem Schlüsselbund gespeichert. Für eine neuerliche Verwendung derselben Schlüssel müssen die Benutzer ihre Passphrase nicht erneut eingeben.
Komplexität des Kennworts	In diesem Feld können Sie die minimale Komplexität von Passphrasen definieren, die für neue Schlüssel verwendet werden sollen. Diese Schlüssel werden am Gerät erzeugt. Sicherere Passphrasen sind immer erlaubt. Sie können folgende Einstellungen auswählen: ▪ **4-Zeichen Kennwort** ▪ **6-Zeichen Kennwort** ▪ **8-Zeichen Kennwort** ▪ **10-Zeichen Kennwort**

Einstellung/Feld	Beschreibung
Egnyte und **WebDAV** Für die Unternehmens-Anbieter können Sie zentral Zugangsdaten definieren. Diese können von den Benutzern nicht geändert werden. Einstellungen, die Sie nicht zentral definieren, können vom Benutzer im entsprechenden App-Dialog eingegeben werden. Beispielsweise können Sie den Server und das Benutzerkonto zentral einstellen, aber das Kennwort-Feld undefiniert lassen. Benutzer müssen dann das Kennwort eingeben, um Zugriff auf den Storage-Anbieter zu bekommen.	
Server	Geben Sie in diesem Feld Folgendes ein: ▪ Die URL zum Root-Ordner am **Unternehmensdokumente** WebDAV-Server ▪ Die URL zum Root-Ordner am **Egnyte**-Server ▪ Die URL zum Root-Ordner am **WebDAV**-Server Verwenden Sie das folgende Format: `https://server.company.com`
Benutzername	Geben Sie in diesem Feld den Benutzernamen für den entsprechenden Server ein.
Kennwort	Geben Sie in diesem Feld das Kennwort für das entsprechende Konto an.
Zielordner	Geben Sie in diesem Feld den Zielordner für das entsprechende Konto an.

Exchange-ActiveSync

In dieser Konfiguration können Sie die Einstellungen für Ihren Microsoft Exchange Server definieren. Sie können mehrere **Exchange-ActiveSync** Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung	Mindestanforderungen
Accountname	Geben Sie in diesem Feld den Accountnamen für das Exchange-ActiveSync Account ein.	

Einstellung/Feld	Beschreibung	Mindestanforderungen
Exchange-ActiveSync-Host	Geben Sie in diesem Feld den Microsoft Exchange Server ein. **Hinweis:** Wenn Sie den SMC EAS Proxy verwenden, geben Sie die URL des SMC Proxy/Servers ein.	✖
Bewegen zulassen	Wenn Sie diese Option deaktivieren, können Benutzer ihre mit diesem Account gesendeten oder erhaltenen Nachrichten nicht in ein anderes Mail Account übertragen. Dies verhindert auch, dass Benutzer ein anderes Konto für das Antworten auf oder das Weiterleiten von Nachrichten aus diesem Konto verwenden.	**5.0+**
Synchronisierung letzter Adressen erlauben	Wenn Sie diese Option deaktivieren, werden kürzlich verwendete Adressen nicht mit anderen Geräten über iCloud synchronisiert.	**6.0+**
Nur mit Mail verwenden	Wenn Sie diese Option auswählen, kann dieses Account nur zum Senden von Mail-Nachrichten verwendet werden. Es kann nicht als Absender-Account für mit anderen Apps erstellten Nachrichten (zum Beispiel Fotos oder Safari) verwendet werden.	**5.0+**
SSL	Wählen Sie diese Option, um für die gesamte Kommunikation SSL (Secure Socket Layer) zu verwenden.	✖
Domain	Geben Sie in diesem Feld die Domäne für Ihre Umgebung an. Sie können dieses Feld auch leer belassen.	✖
Benutzer	Geben Sie in diesem Feld den Benutzer für den Account an. Sie können die Variable %_USERNAME_% verwenden. Der Server ersetzt diese durch den jeweiligen Benutzernamen, wenn für das Gerät, an das das Profil gesendet wird, eine LDAP-Verbindung besteht.	✖
E-Mail-Adresse	Geben Sie in diesem Feld die E-Mail-Adresse für das Account an.	✖

Einstellung/Feld	Beschreibung	Mindestanforderungen
	Sie können die Variable %_EMAILADDRESS_% verwenden. Der Server ersetzt diese durch die jeweilige E-Mail-Adresse, wenn für das Gerät, an das das Profil gesendet wird, eine LDAP-Verbindung besteht.	
Kennwort	Geben Sie in diesem Feld das Kennwort für das Account an.	✖
Zeitraum für die Synchronisierung von E-Mails	Wählen Sie in diesem Feld den Zeitraum für die E-Mail-Synchronisierung. Dabei handelt es sich um die Anzahl an Tagen, für die E-Mails synchronisiert werden. Wenn Sie hier einen Zeitraum angeben, werden nicht alle im Posteingang enthaltenen E-Mails auf dem Mobilgerät synchronisiert, sondern nur die E-Mails aus dem angegebenen Zeitraum. Sie können folgende Optionen auswählen: ▪ **Unbegrenzt** ▪ **Ein Tag** ▪ **Drei Tage** ▪ **Eine Woche** ▪ **Zwei Wochen** ▪ **Ein Monat**	✖
Identitätszertifikat	Wählen Sie in diesem Feld das Identitätszertifikat für die Verbindung zu ActiveSync. Wenn kein Zertifikat zur Auswahl verfügbar ist, wird eine Meldung angezeigt.	✖

WLAN

In dieser Konfiguration geben Sie die Einstellungen für die WLAN-Verbindungen an. Sie können mehrere **WLAN**-Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung	Mindestanforderungen
SSID	Geben Sie in diesem Feld die ID des Drahtlosnetzwerks an.	✖

Einstellung/Feld	Beschreibung	Mindestanforderungen
Automatisch verbinden	Wählen Sie diese Option, um automatisch eine Verbindung mit dem Zielnetzwerk herzustellen.	**5.0+**
Unsichtbares Netzwerk	Wählen Sie diese Option, wenn das Zielnetzwerk nicht offen oder unsichtbar ist.	✖
Sicherheitstyp	In diesem Feld wählen Sie den Sicherheitstyp des WLAN aus: ▪ **Ohne** ▪ **WEP** ▪ **WPA/WPA2** ▪ **Beliebig (persönlich)** ▪ **Firmenweiter WEP** ▪ **Firmenweiter WPA/WPA2** ▪ **Beliebig (firmenweit)** Wenn Sie die persönlichen Einstellungen **WEP**, **WPA/WPA2** oder **Beliebig (persönlich)** wählen, wird ein **Kennwort** Feld angezeigt. Geben Sie das relevante Kennwort ein. Wenn Sie die firmenweiten Einstellungen **Firmenweiter WEP**, **Firmenweiter WPA/WPA2** oder **Beliebig (firmenweit)** wählen, werden die Registerkarten **Protokolle** und **Authentifizierung** angezeigt. Konfigurieren Sie in der **Protokolle** Registerkarte folgende Einstellungen: ▪ Geben Sie unter **Akzeptierte EAP-Typen** die EAP-Verfahren an, die für die Authentisierung verwendet werden sollen. Je nach den hier ausgewählten Typen, lassen sich die Werte im Feld **Innere Identität** (TTLS) auswählen. ▪ Konfigurieren Sie unter **EAP-FAST**, die Einstellungen für die EAP-FAST Protected Access Anmeldedaten. In der **Authentifizierung** Registerkarte legen Sie die Einstellung für die Authentisierung fest: ▪ Geben Sie im **Benutzer** Feld den Benutzernamen für die Verbindung zum Drahtlosnetzwerk ein. ▪ Wählen Sie **Kennwort bei jedem Verbinden abfragen**, wenn das	✖

Einstellung/Feld	Beschreibung	Mindestanforderungen
	Kennwort für jede Verbindung abgefragt und mit der Authentisierung übertragen werden soll. ▪ Geben Sie im **Kennwort** Feld das relevante Kennwort ein. ▪ Wählen Sie im **Identitätszertifikat** Feld das Zertifikat für die Verbindung zum Drahtlosnetzwerk aus. ▪ Geben Sie im **Externe Identität** Feld, die extern sichtbare ID (für TTLS, PEAP und EAP Fast) ein.	
Proxy	Wählen Sie in diesem Feld die Proxy-Einstellungen für die WLAN-Verbindung aus: ▪ **Ohne** ▪ **Manuell** ▪ **Automatisch** Wenn Sie **Manuell** auswählen, werden die Felder **Server und Port**, **Authentifizierung** und **Kennwort** angezeigt. Geben Sie die erforderlichen Proxy-Informationen ein. Wenn Sie **Automatisch** auswählen, wird das Feld **Proxy-Server-URL** angezeigt. Geben Sie die URL des Proxy-Servers ein.	

VPN

In dieser Konfiguration können Sie VPN-Einstellungen für Netzwerke definieren. Sie können mehrere **VPN** Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
Verbindungsname	Geben Sie in diesem Feld den Namen der Verbindung ein, der auf dem Gerät angezeigt wird.
Verbindungstyp	Wählen Sie in diesem Feld den Verbindungstyp: ▪ **Cisco AnyConnect** ▪ **IPSec (Cisco)** ▪ **F5** ▪ **Check Point** ▪ **SSL (benutzerdefiniert)**

Einstellung/Feld	Beschreibung
	Je nach hier gewähltem Verbindungstyp werden in der **VPN** Ansicht unterschiedliche Eingabefelder angezeigt.
Identifier (Reverse-DNS-Format) (Verbindungstyp **SSL (benutzerdefiniert)**)	Geben Sie in diesem Feld die benutzerdefinierte Kennung im Reverse-DNS-Format ein.
Server (alle Verbindungstypen)	Geben Sie in diesem Feld den Host-Namen oder die IP-Adresse des Servers ein.
Account (alle Verbindungstypen)	Geben Sie in diesem Feld das Benutzer-Account für die Authentisierung der Verbindung ein.
Benutzerdefinierte Daten (Verbindungstyp SSL (benutzerdefiniert))	Geben Sie hier benutzerdefinierte Daten ein, die Sie von Ihrem Anbieter erhalten haben: ▪ Klicken Sie **Hinzufügen** und geben Sie **Schlüssel** und **Wert** in der **Benutzerdefinierte Daten** Ansicht ein. ▪ Klicken Sie **Übernehmen**. **Schlüssel** und **Wert** wird in der **VPN** Ansicht angezeigt.
Gruppe (Verbindungstyp **Cisco AnyConnect**)	Geben Sie in diesem Feld die Gruppe ein, die für die Authentisierung der Verbindung erforderlich sein kann.
Alle Daten über das VPN übertragen	Wählen Sie diese Option, wenn der gesamte Datenverkehr über VPN gesendet werden soll.
Benutzer-Authentifizierung (Verbindungstyp **Cisco AnyConnect**, **F5**, **Custom SSL**)	Wählen Sie in diesem Feld die Art der Benutzer-Authentisierung für die Verbindung: ▪ **Kennwort** Wenn Sie diese Option auswählen, wird unter dem **Benutzer-Authentifizierung** Feld ein **Kennwort** Feld angezeigt. Geben Sie das Kennwort für die Authentisierung ein. ▪ **Zertifikat** Wenn Sie diese Option auswählen, wird unter dem **Benutzer-Authentifizierung** Feld ein **Zertifikat** Feld angezeigt. Wählen Sie ein Zertifikat aus.
Geräte-Authentifizierung (Verbindungstyp **IPSec (Cisco)**)	Wählen Sie in diesem Feld die Art der Geräte-Authentisierung: ▪ **Schlüssel (Shared Secret)/Gruppenname**

Einstellung/Feld	Beschreibung
	Wenn Sie diese Option auswählen, werden die Felder **Gruppenname**, **Schlüssel (Shared Secret)**, **Hybrid-Authentifizierung verwenden** und **Kennwort verlangen** unter dem **Geräte-Authentifizierung** Feld angezeigt. Geben Sie die erforderlichen Authentisierungsinformationen in den Feldern **Gruppenname** und **Schlüssel (Shared Secret)** ein. Wählen Sie je nach Anforderung **Hybrid-Authentifizierung verwenden** und **Kennwort verlangen**. ▪ **Zertifikat** Wenn Sie diese Option auswählen, werden die Felder **Zertifikat** und **Inklusive Benutzer-PIN** unter dem **Geräte-Authentifizierung** Feld angezeigt. Wählen Sie im **Zertifikat** Feld das erforderliche Zertifikat aus. Wählen Sie **Inklusive Benutzer-PIN**, um die Benutzer-PIN in die Geräteauthentisierung einzubeziehen.
Proxy (alleVerbindungstypen)	Wählen Sie in diesem Feld die Proxy-Einstellungen für die Verbindung: ▪ **Ohne** ▪ **Manuell** Wenn Sie diese Option wählen, werden die Felder **Server und Port**, **Authentifizierung** und **Kennwort** angezeigt. Geben Sie im **Server und Port** Feld die gültige Adresse und den Port des Proxy-Servers ein. Geben Sie im **Authentifizierung** Feld den Benutzernamen für die Verbindung zum Proxy-Server ein. Geben Sie im **Kennwort** Feld das Kennwort für die Verbindung zum Proxy-Server ein. ▪ **Automatisch** Wenn Sie diese Option wählen, wird das Feld **Proxyserver-URL** angezeigt. Geben Sie die URL des Servers mit der Proxy-Einstellung in diesem Feld ein.

VPN pro App

Mindestanforderung: iOS-Version **7.0+**

In dieser Konfiguration können Sie VPN-Einstellungen für die Unterstützung des iOS-Features "VPN pro App" definieren. Mit diesem Feature lassen sich Apps so konfigurieren, dass sie beim Starten automatisch eine VPN-Verbindung herstellen. Somit können Sie zum Beispiel sicherstellen, das von Managed Apps übermittelte Daten über VPN übertragen werden.

Wenn Sie „VPN pro App“-Konfigurationen eingerichtet haben, können Sie in der Ansicht **Paket bearbeiten** einer App eine Konfiguration auswählen (siehe Konfigurieren von VPN pro App und Einstellungen für iOS-Apps (Seite 111)).

Einstellung/Feld	Beschreibung
Verbindungsname	Geben Sie in diesem Feld den Namen der Verbindung ein, der auf dem Gerät angezeigt wird.
Verbindungstyp	Wählen Sie in diesem Feld den Verbindungstyp: ▪ **Cisco AnyConnect** ▪ **F5** ▪ **Check Point** ▪ **SSL (benutzerdefiniert)** Je nach hier gewähltem Verbindungstyp werden in der **VPN** Ansicht unterschiedliche Eingabefelder angezeigt.
Identifier (Reverse-DNS-Format) (Verbindungstyp **SSL (benutzerdefiniert)**)	Geben Sie in diesem Feld die benutzerdefinierte Kennung im Reverse-DNS-Format ein.
Server (alle Verbindungstypen)	Geben Sie in diesem Feld den Host-Namen oder die IP-Adresse des Servers ein.
Account (alle Verbindungstypen)	Geben Sie in diesem Feld das Benutzer-Account für die Authentisierung der Verbindung ein.
Benutzerdefinierte Daten (Verbindungstyp SSL (benutzerdefiniert))	Geben Sie hier benutzerdefinierte Daten ein, die Sie von Ihrem Anbieter erhalten haben: ▪ Klicken Sie **Hinzufügen** und geben Sie **Schlüssel** und **Wert** in der **Benutzerdefinierte Daten** Ansicht ein. ▪ Klicken Sie **Übernehmen**. **Schlüssel** und **Wert** wird in der **VPN** Ansicht angezeigt.
Gruppe (Verbindungstyp **Cisco AnyConnect**)	Geben Sie in diesem Feld die Gruppe ein, die für die Authentisierung der Verbindung erforderlich sein kann.
Alle Daten über das VPN übertragen	Wählen Sie diese Option, wenn der gesamte Datenverkehr über VPN gesendet werden soll.
Benutzer-Authentifizierung (Verbindungstyp **Cisco AnyConnect**, **F5**, **Custom SSL**)	Wählen Sie in diesem Feld die Art der Benutzer-Authentisierung für die Verbindung: ▪ **Kennwort**

Einstellung/Feld	Beschreibung
	Wenn Sie diese Option auswählen, wird unter dem **Benutzer-Authentifizierung** Feld ein **Kennwort** Feld angezeigt. Geben Sie das Kennwort für die Authentisierung ein. ▪ **Zertifikat** Wenn Sie diese Option auswählen, wird unter dem **Benutzer-Authentifizierung** Feld ein **Zertifikat** Feld angezeigt. Wählen Sie ein Zertifikat aus.
Geräte-Authentifizierung (Verbindungstyp **IPSec (Cisco)**)	Wählen Sie in diesem Feld die Art der Geräte-Authentisierung: ▪ **Schlüssel (Shared Secret)/Gruppenname** Wenn Sie diese Option auswählen, werden die Felder **Gruppenname**, **Schlüssel (Shared Secret)**, **Hybrid-Authentifizierung verwenden** und **Kennwort verlangen** unter dem **Geräte-Authentifizierung** Feld angezeigt. Geben Sie die erforderlichen Authentisierungsinformationen in den Feldern **Gruppenname** und **Schlüssel (Shared Secret)** ein. Wählen Sie je nach Anforderung **Hybrid-Authentifizierung verwenden** und **Kennwort verlangen**. ▪ **Zertifikat** Wenn Sie diese Option auswählen, werden die Felder **Zertifikat** und **Inklusive Benutzer-PIN** unter dem **Geräte-Authentifizierung** Feld angezeigt. Wählen Sie im **Zertifikat** Feld das erforderliche Zertifikat aus. Wählen Sie **Inklusive Benutzer-PIN**, um die Benutzer-PIN in die Geräteauthentisierung einzubeziehen.
Proxy (alleVerbindungstypen)	Wählen Sie in diesem Feld die Proxy-Einstellungen für die Verbindung: ▪ **Ohne** ▪ **Manuell** Wenn Sie diese Option wählen, werden die Felder **Server und Port**, **Authentifizierung** und **Kennwort** angezeigt. Geben Sie im **Server und Port** Feld die gültige Adresse und den Port des Proxy-Servers ein. Geben Sie im **Authentifizierung** Feld den Benutzernamen für die Verbindung zum Proxy-Server ein. Geben Sie im **Kennwort** Feld das Kennwort für die Verbindung zum Proxy-Server ein. ▪ **Automatisch**

Einstellung/Feld	Beschreibung
	Wenn Sie diese Option wählen, wird das Feld **Proxyserver-URL** angezeigt. Geben Sie die URL des Servers mit der Proxy-Einstellung in diesem Feld ein.
Automatische Verbindung bei Bedarf	Wählen Sie dieses Feld um sicherzustellen, dass die VPN-Verbindung automatisch hergestellt wird.

Single Sign-on

Mindestanforderung: iOS-Version **7.0+**

In dieser Konfiguration können Sie Einstellungen für einen Single Sign-on für Drittanbieter-Apps definieren.

Einstellung/Feld	Beschreibung
Name	Ein von Menschen lesbarer Name für den Account.
Kerberos-Principal-Name	Optional. Der Kerberos-Principal-Name. Wird dieser nicht angegeben, so wird der Benutzer während der Profil-Installation zur Eingabe eines Namens aufgefordert.
Realm	Der Kerberos-Realm-Name. Der Realm Name muss in Großbuchstaben angegeben werden.

In der Registerkarte **URLs** können Sie nach Wunsch einen Liste mit URL-Präfixen anlegen, der entsprochen werden muss, damit dieser Account für die Kerberos-Authentisierung über HTTP verwendet werden kann. Wenn Sie hier keine Präfixe angeben, entspricht der Account allen http:// und https:// URLs.

In der Registerkarte **Kennungen** können Sie nach Wunsch eine Liste mit App-Kennungen anlegen, die diese Anmeldung verwenden können. Wenn Sie hier keine App-Kennungen angeben, gilt die Anmeldung für alle Kennungen.

Kioskmodus

Mindestanforderung: iOS-Version **6.0+ supervised**

In dieser Konfiguration können Sie Einstellungen für den Kioskmodus definieren. Dieser Modus sperrt das Benutzergerät so, dass nur eine App verwendet werden kann und verhindert, dass Benutzer zu anderen Apps wechseln.

Einstellung/Feld	Beschreibung	Mindestanforderungen
Quelle wählen	In diesem Feld können Sie die Quelle für die einzelne App auswählen: ▪ Wenn Sie **App-Liste** wählen, wird die **Apps** Dropdown-Liste mit allen für diesen Kunden verfügbaren iOS-Apps angezeigt. Wählen Sie die App aus der Liste aus und klicken Sie auf **Übernehmen**. ▪ Wenn Sie **Benutzerdefiniert** auswählen, wird das Feld **Kennung** angezeigt. Geben Sie die App-Kennung ein und klicken Sie auf **Übernehmen**.	
Optionen		**7.0+**
Touch deaktivieren	Wählen Sie diese Option, um Touch für den Kioskmodus zu deaktivieren.	
Bildschirmrotation deaktivieren	Wählen Sie diese Option, um die Bildschirmrotation für den Kioskmodus zu deaktivieren.	
Lautstärketasten deaktivieren	Wählen Sie diese Option, um die Lautstärketasten für den Kioskmodus zu deaktivieren.	
Lautlos-Schalter deaktivieren	Wählen Sie diese Option, um den Lautlosschalter für den Kioskmodus zu deaktivieren.	
Standby-Taste deaktivieren	Wählen Sie diese Option, um die Standby-Taste für den Kioskmodus zu deaktivieren.	
Automatische Bildschirmsperre deaktivieren	Wählen Sie diese Option, um die automatische Bildschirmsperre für den Kioskmodus zu deaktivieren.	
Voice Over aktivieren	Wählen Sie diese Option, um Voice Over für den Kioskmodus zu aktivieren.	
Zoom aktivieren	Wählen Sie diese Option, um den Zoom für den Kioskmodus zu aktivieren.	
Farben umkehren aktivieren	Wählen Sie diese Option, um das Umkehren von Farben für den Kioskmodus zu aktivieren.	
AssistiveTouch aktivieren	Wählen Sie diese Option, um AssistiveTouch für den Kioskmodus zu aktivieren.	

Einstellung/Feld	Beschreibung	Mindestanforderungen
Vorlesen von ausgewähltem Text aktivieren	Wählen Sie diese Option, um das Vorlesen von ausgewähltem Text für den Kioskmodus zu aktivieren.	
Mono-Audio aktivieren	Wählen Sie diese Option, um Mono-Audio für den Kioskmodus zu aktivieren.	
Vom Benutzer änderbare Optionen		**7.0+**
Voice Over	Wählen Sie diese Option, um die Anpassung von Voice Over zu erlauben.	
Zoomen	Wählen Sie diese Option, um das Zoomen zu erlauben.	
Farben umkehren	Wählen Sie diese Option, um das Umkehren von Farben zu erlauben.	
AssistiveTouch	Wählen Sie diese Option, um die Anpassung von AssistiveTouch zu erlauben.	

Webclip

In dieser Konfiguration können Sie Webclips definieren, die zum Home-Bildschirm der Benutzergeräte hinzugefügt werden. Webclips bieten schnellen Zugriff auf favorisierte Webseiten. Sie können jedoch zum Beispiel auch einen Webclip mit einer Support-Telefonnummer hinzufügen, damit die Benutzer schnell den Helpdesk kontaktieren können. Sie können mehrere **Webclip** Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
Beschreibung	Geben Sie in diesem Feld eine Beschreibung für den Webclip ein.
URL	Geben Sie in diesem Feld die URL des Webclips ein.
Kann entfernt werden	Wenn Sie diese Option deaktivieren, kann der Benutzer den Webclip nicht entfernen. Der Webclip kann nur durch Entfernen des Profils, das den Webclip installiert hat, entfernt werden.
Bildschirmfüllend	Wenn Sie diese Option auswählen, wird der Webclip auf dem Gerät bildschirmfüllend geöffnet. Ein bildschirmfüllender Webclip öffnet die URL als Web App.

APN

Mit dieser Konfiguration können Sie den Name des Zugangspunkts (APN) des Geräts und die Mobilnetzwerk-Proxy-Einstellungen ändern. Diese Einstellungen legen fest, wie sich Geräte mit dem Netzwerk des Anbieters verbinden. Sie können nur eine **APN** Konfiguration in einem Profil hinzufügen.

Hinweis: Wenn diese Einstellungen nicht korrekt sind, kann das Gerät nicht auf Daten über ein Mobilnetzwerk zugreifen. Wenn Sie die Einstellungsänderungen rückgängig machen wollen, müssen Sie das Profil vom Gerät entfernen.

Einstellung/Feld	Beschreibung
Name des Zugangspunkts (APN)	Geben Sie in diesem Feld den Namen des Zugangspunkts des Anbieters (GPRS) ein.
Benutzername für Zugangspunkt	Geben Sie in diesem Feld den Benutzernamen für den Zugangspunkt ein. **Hinweis:** iOS unterstützt Benutzernamen für Zugangspunkte mit bis zu 64 Zeichen.
Kennwort für Zugangspunkt	Geben Sie in diesem Feld das Kennwort für den Zugangspunkt ein. **Hinweis:** iOS unterstützt Kennwörter für Zugangspunkte mit bis zu 64 Zeichen.
Proxy-Server und -Port	Geben Sie in diesem Feld die gültige Adresse und den Port des Proxy-Servers ein.

Webfilter

Mindestanforderung: iOS-Version **7.0+ supervised**

In dieser Konfiguration können Sie URL-Blacklists und Whitelists mit Lesezeichen definieren.

Einstellung/Feld	Beschreibung
Blacklist	Wählen Sie dieses Feld, um eine Liste mit blockierten URLs zu definieren, auf die auf den Benutzerendgeräten nicht zugegriffen werden darf. Klicken Sie auf **Weiter**, um die **Webfilter** Ansicht anzuzeigen. In dieser Ansicht können Sie einzelne URLs hinzufügen. Verwenden Sie eine neue Zeile für jede URL.
Whitelist mit Lesezeichen	Wählen Sie dieses Feld, um eine Whitelist mit Lesezeichen anzulegen, die auf den

Einstellung/Feld	Beschreibung
	Endbenutzergeräten zum Safari-Browser hinzugefügt werden. Alle anderen Websites werden werden gesperrt. Klicken Sie auf **Weiter**, um die **Webfilter** Ansicht anzuzeigen. Klicken Sie auf **Hinzufügen**, um individuelle URLs als Lesezeichen zu definieren.

Globaler HTTP-Proxy

Mindestanforderung: **supervised**

Hinweis: Diese Option ist nur für "Supervised" Geräte wirksam.

Mit dieser Konfiguration können Sie einen einzigen Unternehmens-Proxy Server konfigurieren. Sie können nur eine **Globaler HTTP-Proxy** Konfiguration in einem Profil hinzufügen.

Einstellung/Feld	Beschreibung
Globaler HTTP-Proxy	Wählen Sie in diesem Feld die Proxy-Einstellungen für die Verbindung: ▪ **Manuell** Wenn Sie diese Option wählen, werden die Felder **Server und Port**, **Authentifizierung** und **Kennwort** angezeigt. Geben Sie im **Server und Port** Feld die gültige Adresse und den Port des Proxy-Servers ein. Geben Sie im **Authentifizierung** Feld den Benutzernamen für die Verbindung zum Proxy-Server ein. Geben Sie im **Kennwort** Feld das Kennwort für die Verbindung zum Proxy-Server ein. ▪ **Automatisch** Wenn Sie diese Option wählen, wird das Feld **Proxyserver-URL** angezeigt. Geben Sie die URL des Servers mit der Proxy-Einstellung in diesem Feld ein.

Root-Zertifikat

In dieser Konfiguration können Sie ein Root-Zertifikat für Geräte hochladen. Sie können mehrere **Root-Zertifikat** Konfigurationen hinzufügen. Suchen Sie im **Datei** Feld nach dem relevanten Zertifikat und klicken Sie auf **Übertragen**. Der Name des Zertifikats wird im **Zertifikatsname** Feld angezeigt.

Hinweis: Das hier hochgeladene Zertifikat ist nur für dieses Profil verfügbar. Wenn Sie Zertifikate in anderen Profilen benötigen, müssen Sie diese erneut hochladen.

Client-Zertifikat

In dieser Konfiguration können Sie ein Client-Zertifikat für Geräte hochladen. Sie können mehrere **Client-Zertifikat** Konfigurationen hinzufügen. Suchen Sie im **Datei** Feld nach dem relevanten Zertifikat und klicken Sie auf **Übertragen**. Der Name des Zertifikats wird im **Zertifikatsname** Feld angezeigt. Geben Sie das **Kennwort** für das ausgewählte Zertifikat ein.

Hinweis: Das hier hochgeladene Zertifikat ist nur für dieses Profil verfügbar. Wenn Sie Zertifikate in anderen Profilen benötigen, müssen Sie diese erneut hochladen.

SCEP

In dieser Konfiguration können Sie Einstellungen definieren, die es den Geräten ermöglichen, Zertifikate über Simple Certificate Enrollment Protocol (SCEP) von einer Zertifizierungsstelle (Certificate Authority) zu erhalten. Sie können nur eine **SCEP** Konfiguration in einem Profil hinzufügen.

Hinweis: Diese Konfiguration steht nur dann zur Verfügung, wenn SCEP während der Einrichtung von Sophos Mobile Control konfiguriert wurde. SCEP muss während der Installation von Sophos Mobile Control aktiviert werden, siehe *Sophos Mobile Control Installation Guide* (Englisch). Als Superadministrator können Sie dann die erforderlichen SCEP-Einstellungen in der Web-Konsole konfigurieren, siehe *Sophos Mobile Control Super Administrator Guide* (Englisch). Die definierten Einstellungen werden an iOS-Profile übertragen.

Hinweis: Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt.

Einstellung/Feld	Beschreibung
URL	Geben Sie in diesem Feld die URL des SCEP-Servers ein.
CA-Name	Geben Sie in diesem Feld einen Namen ein, der von der Zertifizierungsstelle verstanden wird. Der Name kann zum Beispiel zur Unterscheidung zwischen Instanzen verwendet werden.
Betreff	Geben Sie in diesem Feld eine Darstellung eines X.500 Namens in Form eines Datenfelds aus OID und Wert ein. Zum Beispiel: /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar. Dies wird wie folgt übersetzt: [[[“C”, “US”]], [[“O”, “Apple Inc.”]], ..., [[“1.2.5.3”, “bar”]]]
Typ des alternativen Namens des Inhabers	Wählen Sie in diesem Feld den Typ des alternativen Namens für den SCEP-Server: ▪ **Ohne** ▪ **RFC 822-Name** (Email-Adresse) ▪ **DNS-Name** ▪ **Uniform Resource Identifier**

Einstellung/Feld	Beschreibung
	Wenn Sie eine andere Option als **Ohne** wählen, werden unter dem Feld **Typ des alternativen Namens des Inhabers** die Felder **Wert des alternativen Namens des Inhabers** und **NT-Benutzeranmeldename** angezeigt. Geben Sie die erforderlichen Namensangaben ein.
Challenge	Geben Sie in diesem Feld ein Pre-Shared Secret ein, anhand dessen der SCEP-Server die Anforderung oder den Benutzer identifizieren kann. **Hinweis:** Wenn das SCEP-Modul des Sophos Mobile Control Server benutzt wird, ist diese Feld mit %_CACHALLENGE_% vorausgefüllt. Ändern Sie diesen Wert nicht.
Wiederholungen	Legen Sie in diesem Feld fest, wie oft das Gerät einen Übertragungsversuch wiederholen soll, wenn der Server als Antwort "Anstehend" sendet.
RetryDelay	Legen Sie in diesem Feld die Wartezeit in Sekunden zwischen den Versuchen fest.
Schlüsselgröße	Wählen Sie in diesem Feld den Schlüsselgröße: ▪ **1024** ▪ **2048**
Als digitale Signatur verwenden	Wählen Sie diese Option, um festzulegen, dass die Verwendung des Schlüssels als digitale Signatur zulässig ist.
Für Verschlüsselung verwenden	Wählen Sie diese Option, um festzulegen, dass die Verwendung des Schlüssels für die Verschlüsselung zulässig ist.
Signatur	Geben Sie in diesem Feld eine hexadezimale Zeichenfolge als Signatur ein.

15.3.3 Importieren von mit der Apple iPhone Configuration Utility erstellten iOS-Profilen

Sie können mit der Apple iPhone Configuration Utility erstellte Profile in die Web-Konsole importieren.

Hinweis: Die Apple iPhone Configuration Utility steht hier zur Installation zur Verfügung:

- Für Windows: http://support.apple.com/kb/DL1466

- Für Mac OS X: http://support.apple.com/kb/DL1465

1. Nachdem Sie ein Profil in der Apple iPhone Configuration Utility erstellt haben, exportieren Sie es (unverschlüsselt und unsigniert) und speichern Sie es auf Ihrem Computer.
2. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Profile** und dann auf **Apple iOS**.

   Die **Profile** Ansicht wird angezeigt.
3. Klicken Sie auf **Profil anlegen** und wählen Sie **Profil importieren**.

   Die **Profil bearbeiten** Ansicht wird angezeigt.
4. Geben Sie einen **Namen** und eine **Version** für das neue Profil ein.
5. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das das Profil gelten soll.
6. Klicken Sie auf **Datei hochladen** und suchen Sie nach der Datei, die Sie auf Ihrem Computer gespeichert haben. Wählen Sie diese aus und klicken Sie auf **Öffnen**.

   Das Profil wird in der **Profil bearbeiten** Ansicht angezeigt.
7. Klicken Sie auf die **Speichern** Schaltfläche.

Das Profil steht für die Übertragung zur Verfügung. Es wird in der **Profile** Ansicht angezeigt.

15.4 Anlegen von Windows Phone 8-Geräten

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Profile** und dann auf **Windows Phone 8**.

   Die **Profile** Ansicht wird angezeigt.
2. Klicken Sie auf **Profil anlegen**.

   Die **Profil bearbeiten** Ansicht wird angezeigt.
3. Geben Sie einen **Namen** und eine **Version** für das neue Profil ein.
4. Geben Sie im Feld **Beschreibung** eine Beschreibung für das Profil ein.
5. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das das Profil gelten soll.
6. Klicken Sie auf die Schaltfläche **Konfiguration hinzufügen**, um Konfigurationen mit Android-/Windows Phone 8-Konfigurationseinstellungen zum Profil hinzuzufügen.

   Die **Verfügbare Konfigurationen** Ansicht wird angezeigt.
7. Wählen Sie die Konfiguration aus, die Sie hinzufügen möchten, und klicken Sie auf **Weiter**.

   Die Einstellungen-Ansicht der Konfiguration wird angezeigt.
8. Definieren Sie die erforderlichen Einstellungen. Eine detaillierte Liste aller verfügbaren Konfigurationen und Einstellungen finden Sie unter Verfügbare Windows Phone 8-Konfigurationen (Seite 96).
9. Klicken Sie auf die **Übernehmen** Schaltfläche, um Ihre Änderungen zu speichern.

   Die Konfiguration wird in der **Profil bearbeiten** Ansicht unter **Konfigurationen** angezeigt.
10. Wenn Sie alle erforderlichen Konfigurationen hinzugefügt haben, klicken Sie auf die **Speichern** Schaltfläche.

Das Profil steht für die Übertragung zur Verfügung. Es wird in der Ansicht **Profile** für **Android** oder **Windows Phone 8** angezeigt.

15.4.1 Verfügbare Windows Phone 8-Konfigurationen

Die folgenden Konfigurationen sind für Windows Phone 8-Profile in der **Verfügbare Konfigurationen** Ansicht verfügbar, wenn Sie ein Profil erstellen oder bearbeiten. Einige Konfigurationen lassen sich in einem Profil nur einmal hinzufügen, andere mehrmals.

Kennwortrichtlinien

In dieser Konfiguration können Sie Kennwortrichtlinien für Geräte definieren. Sie können nur eine **Kennwortrichtlinien** Konfiguration in einem Profil hinzufügen.

Einstellung/Feld	Beschreibung
Kennworttyp	Wählen Sie in diesem Feld die Art des Kennworts, dass Sie definieren möchten: ▪ **Alphanumerisch** ▪ **Alphanumerisch oder numerisch**
Einfache Werte erlauben	Wenn Sie diese Option auswählen, dürfen Benutzer aufeinander folgende oder wiederholte Zeichen in ihrem Kennwort verwenden, zum Beispiel "1111" oder "abcde".
Minimale Länge des Kennworts	Gibt an, wie viele Zeichen ein Kennwort mindestens enthalten muss.
Maximale Anzahl an Fehlversuchen (1 - 999 oder 0)	In diesem Feld können Sie die Höchstanzahl an fehlgeschlagenen Eingabeversuchen für das Kennwort eingeben. Nach Erreichen der Höchstanzahl wird das Gerät zurückgesetzt.
Inaktivitätszeit in Minuten bis zur Abfrage des Kennworts (1 - 9999 oder 0)	In diesem Feld können Sie festlegen, wann (in Minuten) das Gerät nach Nichtbenutzung gesperrt werden soll. Das Gerät lässt sich durch Eingabe des Kennworts entsperren.
Anzahl der letzten Kennwörter, die nicht benutzt werden dürfen (1 - 50 oder 0)	In diesem Feld können Sie festlegen, wie viele alte Kennwörter gespeichert und mit neu definierten Kennwörtern verglichen werden. Wenn ein Benutzer ein neues Kennwort festlegt, wird es nicht akzeptiert, wenn es mit einem bereits benutzten Kennwort übereinstimmt. Wertebereich: 1 bis 50 oder 0 (keine Kennworthistorie).
Maximale Kennwortgültigkeit (1 - 730 Tage oder ohne)	Fordert eine Änderung des Kennworts im angegebenen Intervall. Wertebereich: 0 (keine Kennwortänderung erforderlich) bis 730 Tage.

Einstellung/Feld	Beschreibung
Minimale Anzahl verschiedener Zeichentypen	Gibt an, wie viele nicht-alphanumerische Zeichen (zum Beispiel & oder !) ein Kennwort mindestens enthalten muss.
Festlegen der Toleranzdauer bis zur erneuten Kennworteingabe erlauben	Wenn Sie diese Option auswählen, dürfen Benutzer die Toleranzdauer bis zur erneuten Eingabe des Kennworts festlegen.

Einschränkungen

In dieser Konfiguration können Sie Einschränkungen für Geräte definieren. Sie können nur eine **Einschränkungen** Konfiguration in einem Profil hinzufügen.

Einstellung/Feld	Beschreibung
SD-Karte nicht erlauben	
Unverschlüsseltes Gerät nicht erlauben	
Action Center-Benachrichtigungen auf dem Sperrbildschirm nicht erlauben	
Manuelles Hinzufügen von Nicht-Microsoft-Konten nicht erlauben	Hinzufügen aller Arten von E-Mail-Konten sowie von Exchange-, Office 365- und Outlook.com-Konten nicht erlauben.
Microsoft-Konto-Verbindung nicht erlauben	Das Microsoft-Konto ist das Systemkonto, das für Synchronisierung, Backup und den Store verwendet wird.
Developer-Unlock nicht erlauben	
Windows Store nicht erlauben	
Nativen Browser nicht erlauben	
Kamera nicht erlauben	
Telemetrie	
Sonstiges	
Kopieren und einfügen nicht erlauben	
Cortana nicht erlauben	

Einstellung/Feld	Beschreibung
Als Office-Dateien speichern nicht erlauben	
Bildschirmaufnahme nicht erlauben	
Teilen von Office-Dateien nicht erlauben	
„Sync my settings“ nicht erlauben	
Sprachaufnahmen nicht erlauben	
WLAN	
WLAN nicht erlauben	
Internet Sharing nicht erlauben	
Automatische Verbindung zu WLAN Sense-Hotspots nicht erlauben	
Hotspot-Reporting nicht erlauben	
Manuelle Konfiguration nicht erlauben	
Konnektivität	
NFC nicht erlauben	
Bluetooth nicht erlauben	
USB-Verbindung nicht erlauben	
Roaming und Kosten	
Datenroaming nicht erlauben	
VPN über Mobilfunk nicht erlauben	
VPN-Roaming über Mobilfunk nicht erlauben	
Sicherheit und Privatsphäre	
Bing Vision zum Speichern von Bildern aus der Bing Vision-Suche nicht erlauben	
Verwendung des Standorts bei der Suche nicht erlauben	

Einstellung/Feld	Beschreibung
Manuelle Installation von Root-Zertifikaten nicht erlauben	
Ortung nicht erlauben	Wenn diese Option aktiviert ist, darf Sophos Mobile Control das Gerät nicht lokalisieren.
SafeSearch-Berechtigung	
Deregistrierung	
Zurücksetzen des Geräts durch Benutzer nicht erlauben	
Manuelle MDM-Deregistrierung nicht erlauben	

Exchange-ActiveSync

In dieser Konfiguration können Sie die Einstellungen für Ihren Microsoft Exchange Server definieren. Sie können mehrere **Exchange-ActiveSync** Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
Name	Geben Sie in diesem Feld einen Konto-Namen an.
Server-Adresse	Geben Sie in diesem Feld die Adresse des Microsoft Exchange Servers an. **Hinweis:** Wenn Sie den SMC EAS Proxy verwenden, geben Sie die URL des SMC Proxy/Servers ein.
SSL	Wählen Sie diese Option, um für die gesamte Kommunikation SSL (Secure Socket Layer) zu verwenden.
Domain	Geben Sie in diesem Feld die Domäne für das Account an.
Benutzer	Geben Sie in diesem Feld den Benutzer für den Account an. Sie können die Variable %_USERNAME_% verwenden. Der Server ersetzt diese durch den jeweiligen Benutzernamen, wenn für das Gerät, an das das Profil gesendet wird, eine LDAP-Verbindung besteht.

Einstellung/Feld	Beschreibung
E-Mail-Adresse	Geben Sie in diesem Feld die E-Mail-Adresse für das Account an. Sie können die Variable %_EMAILADDRESS_% verwenden. Der Server ersetzt diese durch die jeweilige E-Mail-Adresse, wenn für das Gerät, an das das Profil gesendet wird, eine LDAP-Verbindung besteht.
Kennwort	Geben Sie in diesem Feld das Kennwort für das Account an.
Synchronisationsintervall	Wählen Sie in diesem Feld den Abstand zwischen den einzelnen Synchronisierungsvorgängen: ▪ **Automatisch** ▪ **Manuell** ▪ **10 Minuten** ▪ **15 Minuten** ▪ **30 Minuten** ▪ **Eine Stunde**
Zeitraum für die Synchronisierung von E-Mails	Wählen Sie in diesem Feld den Zeitraum für die Synchronisierung. Dabei handelt es sich um die Anzahl an Tagen, für die synchronisiert wird. Wenn Sie hier einen Zeitraum angeben, werden nicht alle Eingänge im Posteingang auf dem Mobilgerät synchronisiert, sondern nur die aus dem angegebenen Zeitraum. Sie können folgende Optionen auswählen: ▪ **Unbegrenzt** ▪ **Drei Tage** ▪ **Eine Woche** ▪ **Zwei Wochen** ▪ **Ein Monat**
Inhalte	Wählen Sie in diesem Feld die Inhalte, die synchronisiert werden: ▪ **E-Mail** ▪ **Kontakte** ▪ **Kalender** ▪ **Aufgaben**

Root-Zertifikat

In dieser Konfiguration können Sie ein Root-Zertifikat für Geräte hochladen. Sie können mehrere **Root-Zertifikat** Konfigurationen hinzufügen. Suchen Sie im **Datei** Feld nach dem relevanten Zertifikat und klicken Sie auf **Übertragen**. Der Name des Zertifikats wird im **Zertifikatsname** Feld angezeigt.

Hinweis: Das hier hochgeladene Zertifikat ist nur für dieses Profil verfügbar. Wenn Sie Zertifikate in anderen Profilen benötigen, müssen Sie diese erneut hochladen.

WLAN

In dieser Konfiguration geben Sie die Einstellungen für die WLAN-Verbindungen an. Sie können mehrere **WLAN**-Konfigurationen hinzufügen.

Einstellung/Feld	Beschreibung
SSID	Geben Sie in diesem Feld die ID des Drahtlosnetzwerks an.
Automatisch verbinden	Wenn Sie diese Option auswählen, wird die Verbindung automatisch hergestellt.
Unsichtbares Netzwerk	Wählen Sie diese Option, wenn das Netzwerk verborgen werden soll.
Sicherheitstyp	Wählen Sie den Sicherheitstyp aus der Dropdown-Liste aus. Wenn Sie **WPA-PSK** oder **WPA2-PSK** auswählen, müssen Sie das Kennwort angeben.
Proxy	Wenn Sie **Manuell** aus der Dropdown-Liste auswählen, müssen Sie Server und Port angeben.

15.5 Platzhalter für Profile

Generische Profile können Platzhalter enthalten, die zum Zeitpunkt der Auftragsausführung durch Benutzerdaten ersetzt werden. Sie können folgende Platzhalter in Profilen verwenden:

ActiveDirectory Platzhalter

- %_EMAILADDRESS_%
- %_USERNAME_%

Geräteeigenschaften-Platzhalter:

%_DEVPROP(Eigenschaftsname)_%

Mit diesem Platzhalter können Sie zum Beispiel die IMEI des Geräts angeben: %_DEVPROP(IMEI)_%

15.6 Übertragen von Apple iOS-, Android- oder Windows Mobile-Profilen

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Profile** auf den gewünschten Mobilgerätetyp: **Apple iOS**, **Android** oder **Windows Mobile**.

   Die **Profile** Ansicht für den ausgewählten Mobilgerätetyp wird angezeigt.

2. Klicken Sie auf die **Übertragung** Schaltfläche.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

3. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Wählen Sie einzelne Geräte aus, an die das Profil übertragen werden soll.
   - Klicken Sie auf die **Gruppenauswahl** Schaltfläche, um die **Gerätegruppe(n) wählen** Ansicht zu öffnen. Wählen Sie dann ein oder mehrere Gerätegruppen für die Übertragung des Profils aus.

4. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Die **Profil wählen** Ansicht wird angezeigt.

5. Wählen Sie das Profil aus, das Sie hinzufügen möchten, und klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

6. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
7. Klicken Sie auf die **Fertigstellen** Schaltfläche.

   Die **Auftragsstatus** Ansicht wird angezeigt.

Das Profil wird zum angegebenen Zeitpunkt auf die ausgewählten Geräte übertragen.

15.7 Übertragen von Windows Phone 8-Profilen

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Profile** auf **Windows Phone 8**.

   Die **Profile** Ansicht für Windows Phone 8 wird angezeigt.

2. Klicken Sie auf die **Übertragung** Schaltfläche.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

3. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Wählen Sie einzelne Geräte aus, an die das Profil übertragen werden soll.
   - Klicken Sie auf die **Gruppenauswahl** Schaltfläche, um die **Gerätegruppe(n) wählen** Ansicht zu öffnen. Wählen Sie dann ein oder mehrere Gerätegruppen für die Übertragung des Profils aus.

4. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Die **Profil wählen** Ansicht wird angezeigt.

5. Wählen Sie das Profil aus, das Sie hinzufügen möchten, und klicken Sie auf **Weiter**.

   Die **Bestätigen** Ansicht wird angezeigt.

6. Klicken Sie auf die **Fertigstellen** Schaltfläche.

Das Profil während des nächsten Synchronisierungsvorgangs auf die ausgewählten Geräte übertragen.

15.8 Herunterladen von iOS-, Android- und Windows Phone 8-Profilen aus der Web-Konsole

Sie können die iOS-, Android- und Windows Phone 8-Profile, die Sie konfiguriert haben, aus der Web-Konsole herunterladen. Dies ist zum Beispiel nützlich, wenn Sie die festgelegten Einstellungen an den Sophos Support weitergeben möchten.

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Profile** auf den gewünschten Mobilgerätetyp: **Apple iOS**, **Android** oder **Windows Phone 8**.

   Die **Profile** Ansicht für den ausgewählten Mobilgerätetyp wird angezeigt.

2. Klicken Sie beim gewünschten Profil auf den **Namen**.

   Die **Profil anzeigen** Ansicht wird angezeigt.

3. Klicken Sie auf die **Download** Schaltfläche.

   Ein Dialog für den Download wird angezeigt.

4. Laden Sie das Profil an einen Speicherort Ihrer Wahl herunter.

iOS-Profile werden als .mobileconfig-Dateien (Plist), Android-Profile als .smcprofile-Dateien (XML-Format) und Windows Phone 8-Profile als .windowsphoneconfig-Dateien gespeichert.

16 Mit Auftragspaketen arbeiten

Mit Auftragspaketen können Sie mehrere Aufträge für Mobilgeräte in einer Transaktion bündeln. Somit können Sie alle Aufträge bündeln, die zur vollständigen Registrierung eines Geräts notwendig sind:

- Provisionierung des Geräts
- Anwendung der erforderlichen Richtlinien
- Installation von erforderlichen Applikationen (zum Beispiel Managed Apps für Apple iOS-Geräte)
- Anwendung der erforderlichen Profile

Sie können auch Wipe-Befehle in Auftragspakete einbeziehen, um Geräte, die nicht mehr den Compliance-Regeln entsprechen (zum Beispiel durch Jailbreak oder Root Access), auf Ihren Fabrikzustand zurückzusetzen. Weitere Informationen finden Sie unter Konfigurieren von Geräterichtlinien (Seite 35).

16.1 Erstellen von Auftragspaketen

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Auftragspakete** und wählen Sie **Android** oder **Apple iOS**.

   Die **Auftragspakete** Ansicht wird angezeigt.

2. Klicken Sie auf **Auftragspaket anlegen**.

   Die **Auftragspaket bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen**, eine **Version** und eine Beschreibung ein.

   Hinweis: Pflichtfelder sind mit einem Sternchen (*) markiert.

4. Wählen Sie unter **Betriebssysteme** die Betriebssysteme, für die das neue Auftragspaket gelten soll.
5. Klicken Sie auf die Schaltfläche **Auftrag anlegen**.
6. Wählen Sie den Auftragstyp und klicken Sie auf **Weiter**.

   Die nächste Ansicht hängt vom gewählten Auftragstyp ab. Wenn Sie zum Beispiel den Typ **Profil installieren** ausgewählt haben, wird die Ansicht **Profil installieren** angezeigt.

7. Folgen Sie den Schritten des Assistenten, um den gewünschten Auftrag hinzuzufügen.
8. Wiederholen Sie diesen Vorgang, um weitere Aufträge hinzuzufügen. Beim Hinzufügen neuer Aufträge können Sie Ihre eigenen aussagekräftigen Namen angeben. Diese Auftragsnamen werden während der Installation im Self Service Portal angezeigt. Mit den Sortier-Pfeilsymbolen auf der rechten Seite der Liste **Aufträge** können Sie die Reihenfolge für die ausgewählten Aufträge festlegen.
9. Wenn Sie alle erforderlichen Aufträge zum Auftragspaket hinzugefügt haben, klicken Sie auf die **Speichern** Schaltfläche in der **Auftragspaket bearbeiten** Ansicht.

Das Auftragspaket steht für die Übertragung zur Verfügung. Es wird in der **Auftragspakete** Ansicht angezeigt.

16.2 Duplizieren von Auftragspaketen

Da das Erstellen eines Auftragspakets zeitaufwändig sein kann, können Sie bereits vorhandene Auftragspakete duplizieren. Diese Funktion ist hilfreich, wenn mehrere umfangreiche Auftragspakete mit ähnlichen Aufträgen erforderlich sind. Es müssen dann nur wenige Aufträge gelöscht oder hinzugefügt werden.

Hinweis: Sie können Auftragspakete nur dann duplizieren, wenn sie nicht gleichzeitig bearbeitet werden. Die Kopien werden mit "Copy of" und dem Namen des Originalprofils benannt. Sie können die Namen der Pakete nach Ihren Anforderungen ändern.

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Auftragspakete** und wählen Sie **Android** oder **Apple iOS**.

   Die **Auftragspakete** Ansicht wird angezeigt.

2. Klicken Sie auf das blaue Dreieck neben dem Auftragspaket, das Sie duplizieren möchten, und klicken Sie auf **Duplizieren**.

Das Auftragspaket wird dupliziert und in der **Auftragspakete** Ansicht angezeigt. Sie können das duplizierte Auftragspaket nun bearbeiten. Um das Auftragspaket zu bearbeiten, klicken Sie auf das daneben stehende blaue Dreieck und wählen Sie **Bearbeiten**.

16.3 Übertragen von Auftragspaketen an einzelne Geräte oder Gerätegruppen

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Auftragspakete** und wählen Sie **Android** oder **Apple iOS**.

   Die **Auftragspakete** Ansicht wird angezeigt.

2. Klicken Sie auf das blaue Dreieck neben dem betreffenden Auftrag und dann auf **Übertragen**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

3. In dieser Ansicht haben Sie folgende Möglichkeiten:
   - Wählen Sie einzelne Geräte aus, an die das Auftragspaket übertragen werden soll.
   - Klicken Sie auf **Gerätegruppe(n) wählen**, um die Ansicht **Gerätegruppe(n) wählen** zu öffnen. Wählen Sie dann eine oder mehrere Gerätegruppen für die Übertragung des Auftragspakets aus.

4. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

5. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
6. Klicken Sie auf die **Fertigstellen** Schaltfläche.

   Die **Auftragsstatus** Ansicht wird angezeigt.

Das Auftragspaket wird zum angegebenen Zeitpunkt auf die ausgewählten Geräte übertragen.

17 Mit Apps arbeiten

In der Web-Konsole können Sie unter **Apps** Apps hinzufügen, die auf Geräten installiert werden sollen.

Sie können die auf den Geräten zu installierenden Apps wie folgt zur Verfügung stellen:

- Sie können die App in die Web-Konsole hochladen.
- Sie können einen Link für den Download zur Verfügung stellen.

  Hinweis: Windows Phone 8-Applikationen können nur über einen Link über den Enterprise App Store installiert werden.

Hinweis: Für iOS-Geräte im Supervised-Modus wird die unbeaufsichtigte Installation von Managed Apps unterstützt, wenn das jeweilige Gerät dies zulässt.

17.1 Hochladen von Apps zur Web-Konsole

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Apps** und wählen Sie die Plattform aus, für die Sie die App hinzufügen möchten.

   Die **Softwarepakete** Ansicht wird angezeigt.

2. Klicken Sie auf **App hinzufügen** und wählen Sie **Android-Paket** oder **iOS-Paket**.

   Die Ansicht **Android-Paket bearbeiten** oder **iOS-Paket bearbeiten** wird angezeigt.

3. Geben Sie einen **Namen** und eine **Version** für das neue Paket ein. Das Feld „Name“ ist ein Pflichtfeld. Im Feld **Kennung** können Sie die Kennung für die App eingeben.

   Hinweis: Wenn Ihnen die Kennung nicht genau bekannt ist, belassen Sie dieses Feld leer. Für iOS-Apps wird die Kennung in der Regel automatisch eingegeben.

4. Für iOS, Android- und Windows Phone 8-Geräte können Sie die Applikation über den Enterprise App Store zur Verfügung stellen und sie als empfohlen oder erforderlich definieren. Wählen Sie hierzu im **Empfehlungsstatus** Feld **Empfohlen** oder **Erforderlich**. Wenn Sie **Empfohlen (managed installieren)** oder **Erforderlich (managed installieren)** auswählen, wird die App als Managed Application auf dem Endbenutzergerät gepusht, sobald der Benutzer sie zum Installieren auswählt.
5. Klicken Sie neben **Verfügbar für Gerätegruppe** auf **Anzeigen** und wählen Sie die Gerätegruppen aus, für die die App verfügbar sein soll.
6. Geben Sie im Feld **Beschreibung** eine Beschreibung für das neue Applikationspaket ein.
7. Klicken Sie neben **Betriebssysteme** auf **Anzeigen** und wählen Sie die Betriebssystemversionen, für die das neue Paket gelten soll.

   Hinweis: Bei Samsung Knox-Geräten ist die Option **In Knox-Container installieren** verfügbar. Wählen Sie diese Option aus, wenn die App in einem Knox-Container installiert werden soll. Die Option ist nur sichtbar, wenn ein Knox Advanced-Lizenzschlüssel bei den **Systemeinstellungen** eingegeben wurde.

8. Klicken Sie auf **Datei hochladen**, um das Paket direkt in die Web-Konsole hochzuladen. Suchen Sie nach dem Paket und klicken Sie auf **Öffnen**.
9. Klicken Sie auf die **Speichern** Schaltfläche.

Die App steht für die Installation zur Verfügung. Es wird in der **Softwarepakete** Ansicht angezeigt. Wenn Sie die Software als **Empfohlen** oder **Erforderlich** konfiguriert haben, wird sie im Enterprise App Store des Sophos Mobile Control Client auf dem Endbenutzergerät zum Download angezeigt. Die Benutzer können sie zur Installation auswählen. Der Installationsvorgang läuft ohne oder nur mit sehr geringer Benutzerinteraktion. Weitere Informationen zur Installation von erforderlichen oder empfohlenen Apps finden Sie im *Sophos Mobile Control Benutzerhandbuch*.

17.2 Anlegen von Links zu Apps

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Apps** und wählen Sie die Plattform aus, für die Sie die App hinzufügen möchten.

   Die **Softwarepakete** Ansicht wird angezeigt.

2. Klicken Sie auf **App hinzufügen** und wählen Sie **Android-Link**, **iOS-Link** oder **Windows Phone-Link**.

   Die jeweilige Ansicht zum Bearbeiten der Links wird angezeigt.

   Hinweis: Wenn Sie einen Link für iOS anlegen möchten, klicken Sie auf **In AppStore suchen**. Geben Sie den Namen der App in das Suchfeld ein und klicken Sie auf **Suchen**. Klicken Sie in den Suchergebnissen auf den Namen der App. Die Felder in der Ansicht **iOS-Link bearbeiten** werden automatisch mit den abgerufenen Daten gefüllt.

3. Geben Sie einen **Namen** und eine **Version** für den neuen Link ein. Das Feld „Name“ ist ein Pflichtfeld. Im Feld **Kennung** können Sie die Kennung für die App eingeben.

   Hinweis: Wenn Ihnen die Kennung nicht genau bekannt ist, belassen Sie dieses Feld leer. Für iOS-Apps wird die Kennung in der Regel automatisch eingegeben.

4. Für iOS, Android- und Windows Phone 8-Geräte können Sie die Applikation über den Enterprise App Store zur Verfügung stellen und sie als empfohlen oder erforderlich definieren. Wählen Sie hierzu im **Empfehlungsstatus** Feld **Empfohlen** oder **Erforderlich**. Wenn Sie **Empfohlen (managed installieren)** oder **Erforderlich (managed installieren)** auswählen, wird die App als Managed Application auf dem Endbenutzergerät gepusht, sobald der Benutzer sie zum Installieren auswählt.
5. Klicken Sie neben **Verfügbar für Gerätegruppe** auf **Anzeigen** und wählen Sie die Gerätegruppen aus, für die die App verfügbar sein soll.
6. Geben Sie im Textfeld **Beschreibung** eine Beschreibung für den neuen Link ein.
7. Klicken Sie neben **Betriebssysteme** auf **Anzeigen** und wählen Sie die Betriebssystemversionen, für die das neue Paket gelten soll.

   Hinweis: Bei Samsung Knox-Geräten ist die Option **In Knox-Container installieren** verfügbar. Wählen Sie diese Option aus, wenn die App in einem Knox-Container installiert werden soll. Die Option ist nur sichtbar, wenn ein Knox Advanced-Lizenzschlüssel bei den **Systemeinstellungen** eingegeben wurde.

8.
   - Um einen Android-Link anzulegen, klicken Sie auf **Link für Android erhalten**, suchen Sie in Google Play nach der gewünschten App und öffnen Sie diese. Kopieren Sie den Link in der Web-Adressenzeile Ihres Browsers.
   - Um einen iOS-Link anzulegen, klicken Sie auf **In AppStore suchen** oder verwenden Sie den Apple Link Maker. Um zur Link Maker-Webseite zu gelangen, klicken Sie auf den Link unter dem Textfeld **Link**.
   - Um einen Windows Phone-Link anzulegen, klicken Sie auf **Link für Windows Phone erhalten**, suchen Sie im Windows Phone Store nach der gewünschten App und öffnen Sie diese. Kopieren Sie den Link in der Web-Adressenzeile Ihres Browsers.
9. Fügen Sie den Link in das Textfeld **Link** ein.
10. Klicken Sie auf **Speichern**.

Die App steht für die Installation zur Verfügung. Es wird in der **Softwarepakete** Ansicht angezeigt. Wenn Sie die Software als **Empfohlen** oder **Erforderlich** konfiguriert haben, wird sie im Enterprise App Store des Sophos Mobile Control Client auf dem Endbenutzergerät zum Download angezeigt. Die Benutzer können sie zur Installation auswählen. Der Installationsvorgang läuft ohne oder nur mit sehr geringer Benutzerinteraktion. Weitere Informationen zur Installation von erforderlichen oder empfohlenen Apps finden Sie im *Sophos Mobile Control Benutzerhandbuch*.

17.3 Verwaltung von mit dem Apple Volume Purchase Program erworbenen Apps

Mit dem Apple Volume Purchase Program (VPP) können Sie iOS Apps in großen Mengen kaufen und diese im Unternehmen verteilen. Detaillierte Informationen zur Registrierung und zur Benutzung des Apple Volume Purchase Program finden Sie unter http://www.apple.com/business/vpp/.

17.3.1 Verwaltung von Apple-VPP-Apps auf der Grundlage von Service Token

Wenn eine beim Apple Volume Purchase Programm aufgegebene Bestellung abgeschlossen ist, können Sie einen Service Token (sToken) mit Lizenzen für die erworbenen Apps herunterladen.

Zur Verwaltung von mit dem Apple Volume Purchase Program erworbenen Apps mit Sophos Mobile Control können Sie den Service Token in der Sophos Mobile Control Web-Konsole einrichten. Dieser Service Token wird für die Authentisierung beim Apple Web Service verwendet. Sie können die im Service Token enthaltenen Lizenzen Benutzern zur Verfügung stellen, indem Sie sie dazu einladen, autorisierte Apple-VPP-Benutzer zu werden. Wenn die Benutzer die Einladung angenommen haben, sind sie autorisierte VPP-Benutzer.

Für die Einladung von Benutzern zur VPP-Autorisierung gibt es unterschiedliche Vorgehensweisen. Die Vorgehensweise hängt davon ab, ob Sie die "interne" oder die "externe" Benutzerverwaltung von Sophos Mobile Control anwenden. Die Anleitungen in diesem Abschnitt decken beiden Möglichkeiten ab.

Hinweis: Informationen zur internen und externen Benutzerverwaltung finden Sie im *Sophos Mobile Control Super Administrator Guide*. Wenn Sie Sophos Mobile Control as a Service verwenden, lesen Sie unter Konfigurieren der Self Service Portal Benutzerverwaltung für Sophos Mobile Control as a Service (Seite 26) nach.

Hier die wichtigsten Handlungsschritte für die Verwaltung von mit dem Apple VPP erworbenen Apps auf der Grundlage von Service Token:

1. Einrichten des VPP Service Token in Sophos Mobile Control
2. Einladen von Benutzern

17.3.1.1 Konfigurieren eines VPP-Service-Token (sToken)

Um die Lizenzen für über das Apple Volume Purchase Program erworbene Apps in Sophos Mobile Control zur Verfügung zu stellen, müssen Sie in der Web-Konsole einen VPP-Service-Token (sToken) konfigurieren.

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Setup** und dann auf **Systemeinstellungen**.

   Die **Systemeinstellungen** Ansicht wird angezeigt.

2. Klicken Sie auf der Registerkarte **Apple Volume Purchase Program** unter **VPP-Service-Token (sToken)** auf den Link zum **Apple iTunes VPP Portal**.

   Die Apple **Volume Purchase Program** Website wird angezeigt.

3. Wählen Sie **Business**.

   Die **Business Store Sign In** Seite wird angezeigt.

4. Geben Sie Ihre **Apple ID** und Ihr Kennwort (im Feld **Password**) ein.
5. Wählen Sie auf der nächsten Seite Ihr Account.

   Ihre **Purchase History** Seite wird angezeigt.

6. Um einen VPP-Service-Token zu generieren und ihn in eine Textdatei herunterzuladen, klicken Sie auf die **Download** Schaltfläche unten auf der Seite.

   Es wird ein sToken generiert und in einer Textdatei an Sie geschickt.

7. Speichern Sie die Datei an einem Ort, auf den Sie von der Sophos Mobile Web-Konsole zugreifen können.
8. Klicken Sie in der Sophos Mobile Control Web-Konsole unter **Systemeinstellungen** auf der Registerkarte **Apple Volume Purchase Program** auf **Datei hochladen**. Suchen Sie nach der Service Token-Datei (.vpp token), wählen Sie diese aus und klicken Sie auf **Öffnen**.

   Organisation und **Ablaufdatum** werden automatisch von der importierten Datei übernommen.

9. Geben Sie optional Ihre Apple-ID und den Ländercode ein.
10. Klicken Sie auf die **Speichern** Schaltfläche.

Hinweis: Wenn Sie Ihre Änderungen gespeichert haben, wird der Text des Service Token aus Sicherheitsgründen nicht mehr im Textfeld angezeigt. In dem Feld ist jedoch ersichtlich, dass ein Service Token konfiguriert ist.

17.3.1.2 Apple VPP-Einladungen senden

Sie können einzelne oder alle Benutzer in der Ansicht „Benutzer anzeigen“ zu Apple VPP einladen.

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Benutzer**.

   Die **Benutzer anzeigen** Ansicht wird angezeigt.

2. Sie können alle oder einzelne Benutzer zu Apple VPP einladen.

   a) Um alle Benutzer einzuladen, klicken Sie auf **Benutzer zu Apple VPP einladen**.

Es öffnet sich ein Dialog, in dem Sie gefragt werden, ob Sie alle Benutzer für Apple VPP registrieren möchten.

Klicken Sie auf **Ja**. An jeden Benutzer wird eine Einladungsmail geschickt. Die Benutzer werden darüber informiert, dass ihr Apple iTunes-Konto mit dem Apple Volume Purchase Program verknüpft wird, wenn sie auf den Link in der E-Mail klicken. Danach können sie die von Ihrem Unternehmen lizenzierten Apps installieren und verwenden.

b) Um einen einzelnen Benutzer einzuladen, klicken Sie in der Ansicht **Benutzer anzeigen** auf den betreffenden Benutzernamen.

Die Ansicht **Benutzer anzeigen** wird angezeigt.

Klicken Sie im Bereich **Apple Volume Purchase Program (VPP)** auf **Benutzer zu VPP einladen**.

Es öffnet sich ein Dialog, in dem Sie gefragt werden, ob Sie diesen Benutzer für Apple VPP registrieren möchten.

Klicken Sie auf **Ja**. An den Benutzer wird eine Einladungsmail geschickt. Der Benutzer wird darüber informiert, dass sein Apple iTunes-Konto mit dem Apple Volume Purchase Program verknüpft wird, wenn er auf den Link in der E-Mail klickt. Danach kann er die von Ihrem Unternehmen lizenzierten Apps installieren und verwenden.

Hinweis: Wenn Sie mit einer externen Benutzerverwaltung arbeiten, können Sie auf **Benutzer suchen und zu Apple VPP einladen** klicken und nach dem gewünschten Benutzer suchen.

Die Benutzer können jetzt Ihre lizenzierten Apps verwenden.

17.3.1.2.1 Verwalten von VPP-Benutzern

In der Ansicht **Benutzer anzeigen** für die einzelnen Benutzer wird der Bereich **Apple Volume Purchase Program (VPP)** angezeigt.

Hier stehen folgende Informationen:

- Apple VPP-Benutzerstatus
- Die für den Benutzer verfügbaren Apps

Wenn Sie den Benutzer aus Apple VPP entfernen möchten, klicken Sie auf **VPP-Registrierung löschen**.

Klicken Sie auf **Einladungsmail erneut senden**, um die Einladungs-E-Mail erneut zu senden, wenn der Benutzer die erste E-Mail nicht erhalten hat oder diese verloren gegangen ist.

17.4 Installation von Apps

Voraussetzung: Das zu installierende Paket wurde unter **Apps** erstellt.

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Apps** und wählen Sie **Android**, **Apple iOS** oder **Windows Phone 8**.

   Die **Softwarepakete** Ansicht wird angezeigt.

2. Klicken Sie auf das blaue Dreieck neben der gewünschten App und dann auf **Installieren**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

3. In dieser Ansicht haben Sie folgende Möglichkeiten:
   - Wählen Sie einzelne Geräte aus, auf denen das Softwarepaket installiert werden soll.

- Klicken Sie auf die Schaltfläche **Gerätegruppe(n) wählen**, um die Ansicht **Gerätegruppe(n) wählen** zu öffnen. Wählen Sie dann eine oder mehrere Gerätegruppen für die Installation der Software aus.

4. Klicken Sie auf **Next**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

5. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
6. Klicken Sie auf die **Fertigstellen** Schaltfläche.

Das Softwarepaket wird zum angegebenen Zeitpunkt auf den ausgewählten Geräten installiert.

17.5 Konfigurieren von VPN pro App und Einstellungen für iOS-Apps

Hinweis: VPN pro App und Einstellungen werden ab iOS 7 unterstützt.

Für iOS-Apps können Sie zur Unterstützung der iOS Funktion "Per App VPN" ein VPN pro App auswählen. Mit diesem Feature lassen sich Apps so konfigurieren, dass sie beim Starten automatisch eine VPN-Verbindung herstellen. Sie können außerdem Einstellungen für die App konfigurieren, die auf dem Endbenutzergerät während der App-Installation umgesetzt werden.

Voraussetzungen:

- Damit Sie ein VPN pro App auswählen können, muss eine **VPN pro App**-Konfiguration in einem iOS-Konfigurationsprofil in der Web-Konsole definiert sein (siehe Erstellen von iOS-Profilen in der Web-Konsole (Seite 66) und Verfügbare iOS-Konfigurationen (Seite 67)).
- Damit Sie Einstellungen definieren können, müssen Ihnen der erforderliche Parameter und der Parametertyp bekannt sein.

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Apps** und dann auf **Apple iOS**.

   Die **Softwarepakete** Ansicht wird angezeigt.

2. Klicken Sie auf das blaue Dreieck neben der gewünschten App und dann auf **Bearbeiten**.

   Die **Paket bearbeiten** Ansicht wird angezeigt.

3. Klicken Sie auf die **Anzeigen** Schaltfläche neben dem **Einstellungen und VPN** Feld.

   Die Ansicht **Einstellungen und VPN bearbeiten** wird angezeigt.

4. Wählen Sie die gewünschte Konfiguration aus der **VPN pro App** Dropdown-Liste, um das VPN zu definieren, mit dem sich die App verbinden soll.
5. Um Managed Einstellungen hinzuzufügen, klicken Sie auf **Parameter anlegen**.

   Die **Kondfigurationsparameter** Ansicht wird angezeigt.

6. Konfigurieren Sie in dieser Ansicht Folgendes:
   a) Geben Sie im Feld **Parameter** den erforderlichen Parameter ein, zum Beispiel SMC_URL.
   b) Geben Sie im Feld **Wert** den Parameterwert ein, zum Beispiel smc.sophos.com.
   c) Wählen Sie im Feld **Typ** den Parametertyp: **String**, **Bool**, **Integer** oder **Real**.
   d) Klicken Sie auf die **Übernehmen** Schaltfläche.

      Die Managed-Einstellungen werden in der Ansicht **Einstellungen und VPN bearbeiten** angezeigt.

7. Klicken Sie in der Ansicht **Einstellungen und VPN bearbeiten** auf die Schaltfläche **Übernehmen**.

   Die **Anzeigen** Schaltfläche in der **Paket bearbeiten** Ansicht zeigt die Anzahl an konfigurierten Sets mit Managed Einstellungen.

8. Klicken Sie auf die **Speichern** Schaltfläche.

Das ausgewählte VPN pro App wird angewendet, wenn sich die App mit VPN verbindet. Die Einstellungen werden während der App-Installation auf das Endbenutzergerät übertragen.

17.6 Deinstallation von Apps

Hinweis: Die stille Deinstallation funktioniert bei iOS-Geräten für Managed Apps, die über Sophos Mobile Control verteilt wurden, und bei Windows Phone-Geräten. Bei Android-Geräten ist eine stille Deinstallation nicht möglich.

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Apps** und wählen Sie **Android** oder **Apple iOS**.

   Die **Softwarepakete** Ansicht wird angezeigt.

2. Klicken Sie auf **Deinstallieren**.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

3. In dieser Ansicht haben Sie folgende Möglichkeiten:
   - Wählen Sie einzelne Geräte aus, auf denen das Softwarepaket deinstalliert werden soll.
   - Klicken Sie auf die Schaltfläche **Gerätegruppe(n) wählen**, um die Ansicht **Gerätegruppe(n) wählen** zu öffnen. Wählen Sie dann eine oder mehrere Gerätegruppen für die Deinstallation der Software aus.

4. Klicken Sie auf **Next**.

   Die Ansicht **App wählen** wird angezeigt.

5. Wählen Sie die gewünschte App aus und klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

6. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
7. Klicken Sie auf die **Fertigstellen** Schaltfläche.

Die ausgewählten Anwendungen werden zum angegebenen Zeitpunkt auf den ausgewählten Geräten deinstalliert.

18 Verteilen von Unternehmensdokumenten

Hinweis: Um diese Funktion zu nutzen, benötigen Sie eine **SMC Advanced-Lizenz** für die Verwaltung von Sophos Secure Workspace.

In der Sophos Mobile Control Web-Konsole können Sie Dateien hochladen, damit diese an die Geräte Ihrer Benutzer verteilt werden.

- In der Sophos Mobile Control Web-Konsole verwaltete Dokumente werden automatisch dem **Unternehmensdokumente**-Store von Sophos Secure Workspace hinzugefügt.
- Im **Unternehmensdokumente**-Store auf dem Gerät werden die Kategorien als Ordner angezeigt.
- Wenn Sophos Secure Workspace nicht von Sophos Mobile Control verwaltet wird, ist der **Unternehmensdokumente**-Store nicht sichtbar.
- Auf Dokumente in **Unternehmensdokumente** besteht nur Lesezugriff. Diese können in Sophos Secure Workspace nicht bearbeitet und erneut hochgeladen werden.

So verteilen Sie Unternehmensdokumente:

- Installieren Sie die Sophos Secure Workspace App (siehe Mit Apps arbeiten (Seite 106)).
- Fügen Sie Dokumente in der Sophos Mobile Control Web-Konsole hinzu.

18.1 Hinzufügen von Unternehmensdokumenten

So verteilen Sie Dokumente an Geräte:

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Dokumente**.

   Die Ansicht **Dokumente** wird angezeigt.

2. Klicken Sie auf **Dokument hinzufügen**.

   Die Ansicht **Dokument bearbeiten** wird angezeigt.

3. Geben Sie eine Kategorie für das Dokument ein.
   - Die **Kategorie** ist der Name des Ordners, in dem das Dokument im **Unternehmensdokumente**-Store auf dem Gerät angezeigt wird.
   - Es können mehrere Dateien derselben **Kategorie** zugeordnet sein.
   - Wenn Sie dieses Feld leer lassen, wird die Datei im Root-Ordner von **Unternehmensdokumente** angezeigt.

4. Legen Sie die Einstellungen für das Dokument fest:
   - Aktivieren Sie **In Zwischenablage kopieren**, wenn der Benutzer die Möglichkeit haben soll, das Dokument in die Zwischenablage zu kopieren.
   - Aktivieren Sie **Dokument teilen**, wenn der Benutzer die Möglichkeit haben soll, das Dokument zu teilen.
   - **Dokument offline verwenden**:

     Aktivieren Sie diese Option, damit Benutzer die Möglichkeit haben, einen **Favoriten** für das Dokument anzulegen. Wenn ein Klartext-Dokument aus **Unternehmensdokumente** als **Favorit** markiert ist, wird es verschlüsselt in der Sophos Secure Workspace App gespeichert. Wenn das Teilen des Dokuments erlaubt ist, wird die verschlüsselte Favoriten-Datei automatisch entschlüsselt, bevor sie an andere Apps weitergeleitet wird. Wenn Sie die Optionen in der Sophos Mobile Control Web-Konsole deaktivieren und Benutzer bereits über Offline-Kopien verfügen, wird die in den Secure Workspace **Favoriten** auf den Mobilgeräten gespeicherte Datei automatisch bei der nächsten Synchronisierung entfernt.

5. Klicken Sie auf **Anzeigen** neben **Zugewiesene Gruppen** und wählen Sie die Gruppe aus, die Zugriff auf das Dokument haben soll.
6. Fügen Sie eine Beschreibung für das Dokument hinzu.
7. Klicken Sie auf **Datei hochladen** und suchen Sie nach dem Dokument. Wählen Sie es aus und klicken Sie auf **Öffnen**.
8. Wiederholen Sie diesen Schritt für alle Dokumente, die Sie verteilen möchten.

Das Dokument wird der Dokumentenliste hinzugefügt. Es wird an die Benutzer verteilt, die es sich in der Sophos Secure Workspace App anschauen können.

19 Verwalten von Geräten

In der Web-Konsole unter **VERWALTEN** > **Geräte** und **Gerätegruppen** haben Sie stets einen aktuellen Überblick zu den registrierten Geräten und den Gerätegruppen. Außerdem können Sie eine Reihe von administrativen Aufgaben durchführen. Nachdem Sie Geräte zu Sophos Mobile Control hinzugefügt haben, können Sie zum Beispiel:

- Gerätedetails einsehen und bearbeiten
- E-Mail-Zugriff für Geräte erlauben oder untersagen
- Geräte remote sperren oder entsperren.
- Passcodes/Passwörter von Geräten zurücksetzen
- Geräte bei Verlust oder Diebstahl remote auf den Auslieferungszustand zurücksetzen
- Geräte deregistrieren (Android und iOS)
- Geräte löschen

19.1 Einsehen von Geräten

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die Ansicht **Geräte** wird mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, angezeigt.

2. Klicken Sie beim gewünschten Gerät auf den Namen.

Die **Gerät anzeigen** Ansicht für das ausgewählte Gerät wird angezeigt.

19.1.1 Die Gerät anzeigen Ansicht

In der **Gerät anzeigen** Ansicht werden alle relevanten Informationen für ein einzelnes Gerät angezeigt. Oben in der Ansicht sehen Sie die wichtigsten Geräteinformationen auf einen Blick:

- **Status** (**Managed** oder **Nicht Managed**)
- **Compliant** (**Ja** oder **Nein**)
- **Betriebssystem**
- **E-Mail-Zugriff** (**Ja** oder **Nein**)
- **Letzte Synchronisation**
- **Letzte App-Synchronisation**
- **Eigentümer** (**Firmengerät** oder **Privates Gerät**)
- **Name**
- **Beschreibung**
- **Benutzer**

  Wenn das Gerät über eine LDAP-Verbindung zu einem externen User Directory verfügt, wird hier der entsprechende Benutzername angezeigt.

- **E-Mail-Adresse**
- **Gerätegruppe**
- **Geräte-ID**

Außerdem zeigt die **Gerät anzeigen** Ansicht detaillierte Geräteinformationen in den folgenden Registerkarten. Die angezeigten Registerkarten und Informationen richten sich nach dem Mobilgerätetyp (Plattform).

- **Installierte Profile**

  Zeigt die auf dem Gerät installierten Profile an.

  Hinweis: Für Android-Geräte werden die Profile ab der Sophos Mobile Control Client-Version 3.0 angezeigt.

  Auf dieser Registerkarte steht die Schaltfläche **Profil installieren** zur Verfügung. Über diese Schaltfläche können Sie Profile auf dem Gerät installieren. Sie können auch Profile vom Gerät entfernen, indem Sie auf das **Löschen** Symbol neben dem relevanten Profil klicken.

  In dieser Registerkarte werden auch Provisionierungsprofile aufgelistet.

- **Geräteeigenschaften**

  Zeigt die Geräteeigenschaften wie z. B. Eigenschaften für Modell, Modellname oder Betriebssystemversion an. Bei Android-Geräten werden Smartphones im Root-Zustand ermittelt und die relevante Eigenschaft wird angezeigt. Bei iOS-Geräten werden Smartphones im Jailbroken-Zustand ermittelt. Die relevante Eigenschaft wird in der Ansicht angezeigt.

- **Eigene Eigenschaften**

  Zeigt die eigenen Eigenschaften. Dies sind die Eigenschaften, die Sie selbst anlegen können. Eigene Eigenschaften können zum Beispiel in Platzhaltern verwendet werden, wenn kein Active Directory zur Verfügung steht. Wenn Sie ein Gerät bearbeiten, können Sie hier auch benutzerspezifische Informationen hinzufügen.

- **Interne Eigenschaften**

  Zeigt interne Geräteeigenschaften wie z. B. zugelassener Active Sync-Traffic oder IMEI an.

- **Richtlinienverletzungen**

  Diese Registerkarte wird nur für Geräte angezeigt, die nicht compliant sind. Sie zeigt die Richtlinienverletzungen des Geräts. Klicken Sie auf das **Anzeigen** Lupen-Symbol neben einer Richtlinienverletzung um die **Historie** der Richtlinenverletzung einzusehen.

  Sie können die für das Gerät angezeigten Compliance-Informationen von der **Richtlinienverletzungen** Registerkarte aus aktualisieren. Klicken Sie auf das Symbol **Bearbeiten** auf der Registerkarte **Richtlinienverletzungen** oder auf das Symbol **Neue Aktion hinzufügen** in der Ansicht **Historie**, um den Dialog **Aktion hinzufügen** aufzurufen. In diesem Dialog können Sie Informationen zur Aktion eingeben, die aufgrund einer Compliance-Verletzung durchgeführt wird. Zum Beispiel: Benutzer per E-Mail benachrichtigt.

- **Installation von Apps**

  Zeigt die auf dem Gerät installierte Software.

  Für iOS-Geräte werden in der Spalte **Managed** auf der Registerkarte **Installierte Apps** die Managed Apps angezeigt. Die Managed Apps iOS Funktionalität wurde mit iOS 5.0

eingeführt. Mit Sophos Mobile Control können Sie solche Apps auf IOS-Geräte pushen und sie auch unbemerkt wieder entfernen.

Hinweis: Sophos Mobile Control unterstützt die Managed Apps Funktionalität ab iOS 5.1.

Für Android-Geräte unterscheidet Sophos Mobile Control zwischen System Apps und Apps, die der Benutzer auf dem Gerät installiert hat.

Für Android-Geräte wird das Datenvolumen, das von den einzelnen Apps benutzt wird, angezeigt.

Für iOS-Geräte wird der Speicherplatz angezeigt, den eine App nach der Installation benötigt. Außerdem wird der unter Umständen zusätzlich benötigte Speicherplatz angezeigt. Dieser Speicherplatz ist gegebenenfalls für Downloads, Konfigurationen, Einstellungen usw. erforderlich.

Auf dieser Registerkarte steht oben links in der Ecke die Schaltfläche **Software installieren** zur Verfügung. Mit dieser Schaltfläche können Sie Software auf dem Gerät installieren. Sie können auch Managed Apps von iOS-Geräten entfernen, indem Sie auf das **Löschen** Symbol neben der relevanten App klicken.

- **System-Apps (Android)**

  Zeigt die Android System Software auf dem Gerät an.

  Hinweis: System Software kann nicht vom Gerät entfernt werden.

- **Zertifikate (iOS, Android und Windows Phone 8)**

  Zeigt die auf dem Gerät benutzten Zertifikate an.

- **Scan-Ergebnisse (Android)**

  Diese Registerkarte ist nur dann verfügbar, wenn für den Kunden, bei dem Sie angemeldet sind, die Sophos Mobile Security-Funktionalität zur Verfügung steht. Die Registerkarte zeigt die Ergebnisse des letzten Sophos Mobile Security Scan-Vorgangs auf dem Gerät. Sophos Mobile Security ist eine Security App für Android Mobiltelefone und Tablets, die Geräte vor schädlichen Apps schützt und Endbenutzer beim Erkennen von App-Berechtigungen unterstützt, die unter Umständen ein Sicherheitsrisiko darstellen. Die App kann von der Sophos Mobile Control Web-Konsole verwaltet werden. Für weitere Informationen siehe Verwaltung von Sophos Mobile Security über Sophos Mobile Control (Seite 126).

Von der **Gerät anzeigen** Ansicht können Sie direkt in die **Gerät bearbeiten** Ansicht wechseln. Um das derzeit angezeigte Gerät zu bearbeiten, klicken Sie auf die **Bearbeiten** Schaltfläche.

19.1.2 Anwenden des erweiterten Gerätefilters

Mit dem erweiterten Gerätefilter können Sie die Gerätelisten nach Ihren Anforderungen filtern.

So wenden Sie den Gerätefilter an:

1. Klicken Sie in der Geräte-Ansicht auf die Schaltfläche **Erweiterter Filter** (Lupensymbol) im Header der Web-Konsole.

   Der **Gerätefilter** Dialog wird mit dem Status **Es ist kein Filter aktiv** angezeigt.

2. Im Dialog **Gerätefilter** können Sie Ihre Filterkriterien festlegen.
3. Wenn Sie die erforderlichen Kriterien ausgewählt haben, klicken Sie auf **Filtern**.

Der Filter wird aktiviert und die Geräteliste wird neu geladen. Das Lupensymbol im Header der Web-Konsole ändert seine Farbe von Blau zu Grün. Dadurch wird angezeigt, dass der

Filter aktiv ist. Um den Filter aufzuheben, klicken Sie erneut auf **Erweiterter Filter** und dann im Filterdialog auf **Aufheben**.

Hinweis: Denken Sie daran, Filter manuell wieder aufzuheben, wenn sie nicht mehr benötigt werden. Andernfalls enthalten Listen oder Berichte unter Umständen nicht die erwarteten Ergebnisse.

19.2 Bearbeiten von Geräten

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die **Geräte** Ansicht mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, wird angezeigt.

2. Klicken Sie auf das blaue Dreieck neben dem gewünschten Gerät und dann auf **Bearbeiten**.

   Die **Gerät bearbeiten** Ansicht für das ausgewählte Gerät wird angezeigt.

3. Nehmen Sie die notwendigen Änderungen vor (zum Beispiel Installation oder Entfernen von Software auf der Registerkarte **Installierte Software**). Klicken Sie dann auf die Schaltfläche **Speichern**.

Ihre Änderungen werden auf das bearbeitete Gerät angewendet.

Hinweis: An Eigenschaften vorgenommene Änderungen treten erst in Kraft, wenn Sie auf **Speichern** geklickt haben. Wenn Sie die vorgenommenen Änderungen nicht speichern, haben sie keinerlei Auswirkungen.

19.2.1 Zuweisen eines Benutzers zu einem Gerät

Sie können Benutzer, die mit der internen Benutzerverwaltung verwaltet werden, Geräten zuweisen. Wenn Sie externe Benutzerverwaltung verwenden, können Sie einen Benutzer aus einem externen Benutzerverzeichnis einem Gerät zuweisen.

Hinweis: Das Benutzersverwaltungsverfahren ist kundenspezifisch und wird beim Erstellen des Kunden festgelegt. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

Beachten Sie, dass dies nicht für Sophos Mobile Control as a Service gilt. Superadministratoren werden für Sophos Mobile Control as a Service nicht unterstützt. Informationen darüber, wie Sie die Methoden für die Benutzerverwaltung für Sophos Mobile Control as a Service festlegen, finden Sie unter Konfigurieren der Self Service Portal Benutzerverwaltung für Sophos Mobile Control as a Service (Seite 26).

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die **Geräte** Ansicht mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, wird angezeigt.

2. Klicken Sie auf das blaue Dreieck neben dem gewünschten Gerät und dann auf **Bearbeiten**.

   Die **Gerät bearbeiten** Ansicht für das ausgewählte Gerät wird angezeigt.

3. Klicken Sie auf die Schaltfläche **Aktionen** und dann auf **Benutzer zuordnen**.

   Die **Suchparameter für Benutzer eingeben** Ansicht wird angezeigt.

4. Geben Sie in den Feldern **Common Name (CN)** und/oder **E-Mail-Adresse** einen Suchparameter ein, zum Beispiel den gesamten Benutzernamen oder einen Teil davon.

   Die **Datensatz wählen** Ansicht wird angezeigt.

5. Wählen Sie den gewünschten Benutzer aus und klicken Sie auf **Weiter**.

   Die **Detailfelder wählen** Ansicht wird angezeigt.

6. Wählen Sie die erforderliche **E-Mail-Adresse** und den **Benutzernamen** aus und klicken Sie auf **Übernehmen**.

   Die **Gerät bearbeiten** Ansicht wird wieder angezeigt.

7. Klicken Sie auf die **Speichern** Schaltfläche.

Hinweis: Das Gerät wird für den relevanten Benutzer im Self Service Portal angezeigt.

19.2.2 Definieren eigener Eigenschaften für Geräte

Wenn Sie ein Gerät auf der Grundlage einer Vorlage erstellen oder ein Gerät bearbeiten, können Sie eigene Eigenschaften definieren, zum Beispiel Systemprozesse.

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die **Geräte** Ansicht mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, wird angezeigt.

2. Klicken Sie auf das blaue Dreieck neben dem gewünschten Gerät und dann auf **Bearbeiten**.

   Die **Gerät bearbeiten** Ansicht für das ausgewählte Gerät wird angezeigt.

3. Gehen Sie zur Registerkarte **Eigene Eigenschaften** und klicken Sie auf die Schaltfläche **Neue Eigenschaft hinzufügen**.

   Die **Eigenschaft bearbeiten** Ansicht wird angezeigt.

4. Geben Sie einen **Namen** und einen **Wert** für die neue eigene Eigenschaft ein.
   Zum Beispiel für Systemprozesse:

   - Name: SystemProcess2
   - Value: Internet;10008d39,BrowserNG.exe

   Für Systemprozesse lautet der **Name** immer "SystemProcess" gefolgt von einem bei "0" beginnenden Index. Leerzeichen sind nicht zulässig. Wenn Sie einen weiteren Prozess anlegen, verwenden Sie den folgenden Index, zum Beispiel "SystemProcess1", "SystemProcess2" usw.

   Die Syntax für **Wert** lautet: <Anzeigename>;<UID des Prozesses <Name des Prozesses>.

   Sie können auch mehrere Prozesse kombinieren, zum Beispiel: <Anzeigename>;<UID des Prozesses>,<Name des Prozesses>;<UID des Prozesses>,<Name des Prozesses>.

5. Klicken Sie auf die **Übernehmen** Schaltfläche.

   Die neue Eigenschaft wird in der **Gerät bearbeiten** Ansicht in der **Eigene Eigenschaften** Registerkarte angezeigt.

6. Klicken Sie auf die **Speichern** Schaltfläche.

19.3 Deregistrieren von Geräten

Sie können durch Sophos Mobile Control verwaltete Android- und iOS-Geräte deregistrieren, wenn sie nicht mehr benutzt werden, z. B. wenn der Benutzer ein neues Gerät erhält. Dies

ist unter anderem nützlich, wenn Sie die Anzahl an Geräten, die ein Benutzer über das Self Service Portal registrieren kann, begrenzt haben.

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die **Geräte** Ansicht mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, wird angezeigt.

2. Klicken Sie auf das blaue Dreieck neben dem gewünschten Gerät und dann auf **Bearbeiten**.

   Die **Gerät bearbeiten** Ansicht für das ausgewählte Gerät wird angezeigt.

3. Klicken Sie die **Aktionen** Schaltfläche und dann auf **Deregistrieren**

   Eine Meldung wird angezeigt, die Sie zur Bestätigung des Deregistrierungsvorgangs auffordert.

4. Klicken Sie auf **Ja**.

Das Gerät wird deregistriert. Dadurch werden folgende Vorgänge ausgelöst:

Android-Geräte:

- Der Sophos Mobile Control Geräteadministrator wird deaktiviert.
- Die Server-Anmeldedaten und alle weiteren erhaltenen Daten werden entfernt.

Apple iOS-Geräte:

- Alle Profile werden entfernt.
- Alle Managed Apps werden entfernt (ab iOS 5.1).
- Die Sophos Mobile Control iOS Client App wird entfernt, falls Sie über Managed Apps (ab iOS 5.1) installiert wurde.
- Alle über Mobile Device Management erhaltenen Zertifikate werden entfernt.

19.4 Gerätegruppen

Gerätegruppen dienen zur Kategorisierung von Geräten. Sie können Geräte zu Gerätegruppen zuweisen, wenn Sie sie zum Sophos Mobile Control Device Management manuell oder über Import hinzufügen. Die Gerätegruppe für ein Gerät lässt sich durch Bearbeiten des Geräts ändern. Ein Gerät gehört jeweils immer exakt zu einer Gerätegruppe. Wir empfehlen, Geräte zu gruppieren. Da sich Aufgaben auch bei Gerätegruppen statt bei Einzelgeräten ausführen lassen, können Sie Geräte so effizient verwalten.

Hinweis: Wir empfehlen, nur Geräte mit demselben Betriebssystem zu gruppieren. Gruppen lassen sich dadurch leichter für Installationen und andere betriebssystemspezifische Vorgänge verwenden.

Für weitere Informationen zum Erstellen von Gerätegruppen, siehe Erstellen von Gerätegruppen (Seite 40).

Hinweis: Wenn Sie eine Gerätegruppe löschen, werden die Mitglieder der Gruppe in eine andere Gruppe verschoben. Diese muss angegeben werden. Ist keine Gruppe mehr vorhanden, in die die Geräte verschoben werden können, so kann die Gruppe nicht gelöscht werden. Bevor eine Gruppe gelöscht wird, wird eine Warnungsmeldung angezeigt.

20 Provisionieren von Geräten über die Sophos Mobile Control Web-Konsole

Nachdem Sie die Geräte in der Web-Konsole hinzugefügt haben, müssen sie mit der Sophos Mobile Control Client-Komponente provisioniert werden. Die Web-Konsole bietet folgende Möglichkeiten für die Provisionierung von Geräten:

- Sie können einzelne, unmanaged Geräte provisionieren, indem Sie den SMC-Client mit der Funktion **Geräte** installieren. Weitere Informationen finden Sie unter Einrichten einzelner Geräte (Seite 121).

Für die effiziente Provisionierung von mehreren Geräten, werden folgende Methoden empfohlen:

- Sie können alle Aufträge, die für die vollständige Registrierung und Provisionierung von Geräten notwendig sind, bündeln, indem Sie Auftragspakete für die Provisionierung der Geräte, die Anwendung der erforderlichen Richtlinien und die Installation der erforderlichen Anwendungen (zum Beispiel Managed Apps für Apple iOS-Geräte) erstellen. Weitere Informationen finden Sie unter Mit Auftragspaketen arbeiten (Seite 104).
- Sie können Geräte von ihren Endbenutzern über das Self Service Portal registrieren und provisionieren lassen. Nehmen Sie hierzu bei der Konfiguration der Einstellungen für die Benutzung des Self Service Portal ein Auftragspaket für die Provisionierung auf. Weitere Informationen dazu, wie Sie die für die Provisionierung erforderlichen Auftragspakete erstellen, finden Sie in der *Sophos Mobile Control Startup-Anleitung* bzw. in der *Sophos Mobile Control as a Service Startup-Anleitung*. Für weitere Informationen zum Auswählen des Auftragspakets in den Self Service Portal Einstellungen siehe Konfigurieren von Self Service Portal Einstellungen (Seite 23). Weitere Informationen zur Benutzung des Self Service Portal finden Sie im *Sophos Mobile Control Benutzerhandbuch.*

20.1 Einrichten einzelner Geräte

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die **Geräte** Ansicht wird angezeigt.

2. Wählen Sie das gewünschte Gerät aus, klicken Sie auf **Aktionen** und dann auf **Einrichten**.

   Hinweis: Sie können mehrere Geräte zum Einrichten auswählen.

3. Klicken Sie auf **Ja**, wenn Sie gefragt werden, ob Sie die ausgewählten Geräte einrichten möchten.

Der Einrichtungsauftrag wird gestartet und in der **Auftragsansicht** angezeigt. Der Benutzer erhält eine E-Mail mit Anweisungen zur Installation der Sophos Mobile Control App auf dem Mobilgerät.

20.2 Provisionieren einzelner Windows Mobile-Geräte

1. Klicken Sie in der Web-Konsolen-Menüleiste unter **Einstellungen** auf **Client-Pakete**.

   Die **Sophos Mobile Control-Client Pakete** Ansicht wird angezeigt.

2. Klicken Sie auf die **Übertragung** Schaltfläche.

   Die **Gerät(e) wählen** Ansicht wird angezeigt.

3. In dieser Ansicht haben Sie folgende Möglichkeiten:

   - Wählen Sie einzelne Geräte aus, auf denen das Client-Paket installiert werden soll.
   - Klicken Sie auf die **Gruppenauswahl** Schaltfläche, um die **Gerätegruppe(n) wählen** Ansicht zu öffnen. Wählen Sie dann ein oder mehrere Gerätegruppen für die Installation des Client-Pakets aus.

4. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**.

   Die **Software wählen** Ansicht wird angezeigt.

5. Wählen Sie das Client-Paket aus, das Sie installieren möchten, und klicken Sie auf **Weiter**.

   Die **Ausführungszeit wählen** Ansicht wird angezeigt.

6. Wählen Sie unter **Auftragsdatum** die Option **Sofort** oder geben Sie ein **Datum** und eine **Uhrzeit** für die Ausführung an.
7. Wählen Sie die Option **Ausführung erzwingen**, um die Installation für die ausgewählten Geräte zu erzwingen.
8. Klicken Sie auf die **Fertigstellen** Schaltfläche.

Bei dem ausgewählten Gerät wird zum angegebenen Zeitpunkt die Ersteinrichtung ausgeführt. Nach dem erfolgreichen Abschluss dieses Vorgangs und der Synchronisierung mit dem Server wird der Gerätestatus mit **Managed** angegeben.

21 Administratoren anlegen

1. Gehen Sie in der Web-Konsole zu **SYSTEM** und klicken Sie auf **Setup** und dann auf **Administratoren**.

   Die **Administratoren anzeigen** Ansicht wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Administrator anlegen**.

   Die **Administrator bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Loginnamen** für den neuen Benutzer ein.
4. Wählen Sie im Feld **Rolle** die Benutzerrolle:

   - **Administrator**
   - **User**
   - **Helpdesk**

   Weitere Informationen finden Sie unter Web-Konsolen-Benutzer (Seite 9).

5. Geben Sie den **Nachnamen** und den **Vornamen** des neuen Benutzers ein.
6. Geben Sie die **E-Mail** Adresse des neuen Benutzers ein.
7. Geben Sie ein einmal zu verwendendes **Kennwort** für die erste Anmeldung an der Web-Konsole ein und bestätigen Sie dieses.
8. Klicken Sie auf die **Speichern** Schaltfläche.

Der neue Benutzer wird angelegt und in der **Administratoren anzeigen** Ansicht angezeigt. Geben Sie die Benutzeranmeldedaten (Benutzer, Kunde und einmal zu verwendendes Kennwort) an den neuen Benutzer weiter. Der neue Benutzer kann sich an der Web-Konsole anmelden und wird zum Ändern seines Kennworts aufgefordert.

22 Senden von Nachrichten an Geräte

Von der Web-Konsole aus können Sie benutzerdefinierte Nachrichten an verwaltete Geräte schicken. Nach dem Bootstrap eines iOS-Geräts und der Installation der Sophos Mobile Control App werden APNs-Nachrichten gesendet. Nach dem Einrichten eines Android-Geräts werden GCM Push-Nachrichten gesendet.

22.1 Senden von Nachrichten an einzelne Geräte

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die **Geräte** Ansicht wird angezeigt.

2. Klicken Sie auf das blaue Dreieck neben dem gewünschten Gerät und dann auf **Bearbeiten** oder klicken Sie auf dessen Namen.

   Die **Gerät anzeigen** oder **Gerät bearbeiten** Ansicht wird angezeigt.

3. Klicken Sie auf **Aktionen** und dann auf **Nachricht senden**.

   Der Dialog **Mitteilungstext eingeben** wird angezeigt.

4. Geben Sie im Textfeld die gewünschte Mitteilung ein. Ein Zeichenzähler unterhalb des Textfelds zählt von der Gesamtzahl der verfügbaren Zeichen bis 0 herunter. Wenn der Wert 0 erreicht ist, können Sie keine weiteren Zeichen mehr eingeben.
5. Klicken Sie auf die **Fertigstellen** Schaltfläche.

23 Lizenzen für die Verwaltung von Sophos Mobile Security und Sophos Secure Workspace

Für die Verwaltung der Sophos Mobile Security App und Sophos Secure Workspace App über Sophos Mobile Control ist eine gültige Lizenz erforderlich. Nach dem Erwerb erhalten Sie einen SMC Advanced-Lizenzschlüssel zur Aktivierung der Lizenzen für Sophos Mobile Security und Sophos Secure Workspace. Wie Sie die Lizenz in der Web-Konsole aktivieren, hängt vom Installationstyp für Sophos Mobile Control (lokale Installation oder Software as a Service) ab.

23.1 Aktivierung von Lizenzen für lokale Installationen

Für lokale Sophos Mobile Control Installationen werden SMC Advanced-Lizenzen vom Superadministrator in der Kundenverwaltung verwaltet. Weitere Informationen finden Sie im *Sophos Mobile Control Super Administrator Guide* (Englisch).

23.2 Aktivieren von Lizenzen für Software as a Service Installationen

1. Klicken Sie in der Web-Konsole unter **SYSTEM** auf **Systemeinstellungen**.

   Die **Systemeinstellungen** Ansicht wird angezeigt.

2. Geben Sie auf der Registerkarte **Lizenz** im Feld **Lizenzschlüssel** den von Sophos erhaltenen Lizenzschlüssel ein und klicken Sie auf **Aktivieren**.

Die **SMC Advanced-Lizenz** für die Verwaltung der Sophos Mobile Security App und Sophos Secure Workspace App wird aktiviert. Das **Aktiver Lizenzschlüssel** Feld zeigt den aktivierten Lizenzschlüssel. Das **Anzahl von Lizenzen** Feld zeigt die Anzahl an verfügbaren Benutzern. Das **Gültig bis** Feld zeigt das Lizenzablaufdatum.

24 Verwaltung von Sophos Mobile Security über Sophos Mobile Control

Sophos Mobile Security ist eine Security App für Android Mobiltelefone und Tablets, die Geräte vor schädlichen Apps schützt und Endbenutzer beim Erkennen von App-Berechtigungen unterstützt, die unter Umständen ein Sicherheitsrisiko darstellen. Seine Webfilter-Funktion erlaubt Ihnen, Webseiten nach Kategorien zu filtern und unpassende Inhalte zu blockieren.

Sophos Mobile Security Management ist ein optionales Modul von Sophos Mobile Control. Zum Verwalten der Sophos Mobile Security App von Sophos Mobile Control aus muss eine SMC Advanced-Lizenz verfügbar sein. Diese Lizenz muss in der Sophos Mobile Control Web-Konsole aktiviert werden.

So verwalten Sie die Sophos Mobile Security App auf Managed-Geräten über die Sophos Mobile Control Web-Konsole:

- Sie können Einstellungen für die Sophos Mobile Security App auf allen Managed-Endbenutzergeräten remote und zentral in der Web-Konsole konfigurieren.
- Sie können sicherstellen, dass die Sophos Mobile Security App auf Endbenutzergeräten installiert ist und in festgelegten Intervallen Scans durchführt. Sie können dies als Compliance-Kriterium definieren.
- Sie können Scans bei bestimmten Geräten auslösen.
- Sie können die Scan-Ergebnisse für Geräte in der Web-Konsole einsehen.

Weitere Informationen zu Sophos Mobile Security finden Sie in der *Sophos Mobile Security Hilfe*.

24.1 Konfigurieren von Antivirus Einstellungen für Sophos Mobile Security

Voraussetzung: Eine SMC Advanced-Lizenz ist verfügbar.

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Profile** und dann auf **Android**.

   Die **Profile** Ansicht wird angezeigt.

2. Klicken Sie auf **Profil anlegen** und wählen Sie **Geräteprofil anlegen**.

   Die **Profil bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Version** für das neue Profil ein.
4. Geben Sie im Feld **Beschreibung** eine Beschreibung für das Profil ein.
5. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das das Profil gelten soll.
6. Klicken Sie auf **Konfiguration hinzufügen**.

   Die **Verfügbare Konfigurationen** Ansicht wird angezeigt.

7. Wählen Sie **Antivirus** und klicken Sie auf **Weiter**.

   Die Einstellungen-Ansicht der Konfiguration wird angezeigt.

8. Wechseln Sie in die **Antivirus** Registerkarte.

9. Unter **Allgemein** können Sie folgende Einstellungen festlegen:

   a) Legen Sie im **Cloud Scan-Modus** Feld fest, wann Sophos Mobile Security einen Scan nach den aktuellen Malware-Informationen durchführen soll. Wählen Sie eine der folgenden Optionen, um festzulegen, wann die Anwendung eine Cloud-Abfrage nutzen soll:

   - **Immer**
   - **Nicht beim Roaming**
   - **Nur WLAN**

   Mit dieser Einstellung lässt sich der Datenverkehr der Anwendung steuern. Wenn Sie den **Cloud Scan-Modus** auf **Nur WLAN** einstellen, wird die Cloud-Abfrage nur dann durchgeführt, wenn das Gerät eine WLAN-Verbindung hat. Wenn Sie den **Cloud Scan-Modus** auf **Nicht beim Roaming** einstellen, wird keine Cloud-Abfrage durchgeführt, während das Gerät einen Roaming-Vorgang in einem fremden Netzwerk durchführt.

   b) Legen Sie im **Scan-Intervall** Feld fest, wie oft Scans ausgeführt werden sollen.

10. Unter **Ziele** können Sie folgende Einstellungen festlegen:

    a) Wählen Sie **System Apps scannen**, um System Apps in die Scan-Vorgänge einzubeziehen.

    System Apps werden standardmäßig nicht gescannt, da diese durch das Android-Betriebssystem geschützt sind und nicht vom Benutzer entfernt werden können. Sie können jedoch hier das Scannen von System Apps aktivieren.

    b) Wenn Sie **Scanne SD-Karte, USB, ...** wählen, werden neben dem standardmäßigen Scan aller auf dem Gerät installierten Anwendungen auch alle Dateien auf SD-Karten, USB und anderen Speichermedien gescannt.

11. Unter **PUAs** können Sie Folgendes auswählen:

    a) Wenn Sie **PUAs erkennen** wählen, wird ein Scan-Vorgang nach PUAs (Potentially Unwanted Applications) durchgeführt.

    Potenziell unerwünschte Apps (PUAs) sind Apps, die zwar nicht schädlich sind, jedoch für Unternehmensnetzwerke als ungeeignet angesehen werden. Dazu gehören beispielsweise Adware, Dialer (Einwahlprogramme), Systemmonitore, Remote-Verwaltungs- und Hacking-Tools. Einige Apps, die unter PUAs fallen, können für manche Benutzer jedoch hilfreich sein.

    Wenn Sie diese Option wählen, erkennt Sophos Mobile Security potenziell unerwünschte Apps im Rahmen von Scan-Vorgängen und benachrichtigt den Benutzer entsprechend.

    b) Wählen Sie **Benutzer darf Apps erlauben**, damit die Benutzer Apps erlauben können, obwohl diese als Malware erkannt wurden. Der Benutzer kann diese Apps als ignoriert kennzeichnen. In nachfolgenden Scans werden diese Apps nicht als PUAs angezeigt.

12. Unter **Apps mit niedriger Reputation** können Sie definieren, wie mit derartigen Apps umgegangen werden soll. Die Klassifizierung von Apps basiert auf Sophos Live Protection Daten. Unter **Modus** können Sie folgende Einstellungen festlegen:

    a) Wählen Sie **Erlauben**, um das Scannen nach Apps niedriger Reputation auszuschalten.

    b) Wählen Sie **Warnen**, um eine Warnung am Gerät anzuzeigen, wenn eine App niedriger Reputation erkannt wurde. Die Benutzer können dann wählen, wie die App behandelt

werden soll. Sie können sie zu einer Liste von erlaubten Apps hinzufügen, so dass keine weiteren Warnungen angezeigt werden, wenn diese App erkannt wird.

c) Wählen Sie **Blockieren** um zu verhindern, dass Apps niedriger Reputation gestartet werden. Eine Warnung wird angezeigt, und der Benutzer kann die App nicht starten.

13. Unter **Echtzeitschutz** können Sie folgende Einstellungen festlegen:

a) Wählen Sie **Scan-Benachrichtigungen**, um Scan-Benachrichtigungen auf dem Gerät zu erhalten.

b) Wählen Sie **SD-Karte überwachen**, um die SD-Karte auf Änderungen zu überprüfen. Wenn neue Dateien auf der SD-Karte gespeichert werden, werden diese gescannt.

14. Wenn die Scanergebnisse Apps enthalten, die gestartet werden dürfen, können Sie diese zur Liste der erlaubten Apps hinzufügen. Apps auf dieser Liste dürfen immer auf den Geräten gestartet werden. Die Apps werden nicht gemeldet.

Sie können solche Apps anhand der Scanergebnisse von Sophos Mobile Security identifizieren (siehe Einsehen von Sophos Mobile Security Scan-Ergebnissen (Seite 130)).

15. Um erlaubte Apps hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie die gewünschte App aus der **App-Liste** aus oder klicken Sie auf **Benutzerdefiniert** und geben Sie manuell **App-Name** und **Kennung** ein.
16. Klicken Sie auf die **Übernehmen** Schaltfläche.

24.2 Konfigurieren von Webfilter-Einstellungen für Sophos Mobile Security

Voraussetzung: Eine SMC Advanced-Lizenz ist verfügbar.

Die Sophos Mobile Security App schützt Sie vor Internetseiten mit schädlichem, unerwünschtem oder illegalem Inhalt.

Hinweis: Dies funktioniert nur mit dem integriertem Browser und Google Chrome.

1. Klicken Sie in der Web-Konsole unter **KONFIGURIEREN** auf **Profile** und dann auf **Android**.

   Die **Profile** Ansicht wird angezeigt.

2. Klicken Sie auf **Profil anlegen** und wählen Sie **Geräteprofil anlegen**.

   Die **Profil bearbeiten** Ansicht wird angezeigt.

3. Geben Sie einen **Namen** und eine **Version** für das neue Profil ein.
4. Geben Sie im Feld **Beschreibung** eine Beschreibung für das Profil ein.
5. Wählen Sie unter **Betriebssysteme** das Betriebssystem, für das das Profil gelten soll.
6. Klicken Sie auf die Schaltfläche **Konfiguration hinzufügen**.

   Die **Verfügbare Konfigurationen** Ansicht wird angezeigt.

7. Wählen Sie **Webfilter** und klicken Sie auf **Weiter**.

   Die Einstellungen-Ansicht der Konfiguration wird angezeigt.

8. Legen Sie im Feld **Filtere schädliche Webseiten** fest, ob Sie schädliche Webseiten **Erlauben** wollen, ob Sie den Benutzer **Warnen** wollen, oder ob Sie schädliche Webseiten **Blockieren** wollen.

9. Unter **Websites nach Kategorien filtern** legen Sie für jede Kategorie fest, ob Sie den Zugriff auf Webseiten dieser Kategorie **Erlauben** wollen, ob Sie den Benutzer **Warnen** wollen, oder ob Sie Webseiten mit möglicherweise schädlichem, unerwünschtem oder illegalem Inhalt **Blockieren** wollen.

   Webseiten werden basierend auf Daten von SophosLabs kategorisiert. Die Daten werden laufend aktualisiert.

10. Unter **Website-Ausschlüsse** können Sie Folgendes festlegen:

    a) **Erlaubte URLs**: Fügen Sie URLs hinzu, die erlaubt sind, auch wenn die Kategorie, zu der sie gehören, blockiert wird.

    b) **Blockierte URLs**: Fügen Sie URLs hinzu, die blockiert werden, auch wenn die Kategorie, zu der sie gehören, erlaubt wird.

    Sie können Host-Namen oder IP-Adressen eingeben. Beispiel: www.company.com, *.company.com, 10.2.0.1, 10.2.0.1/24

11. Klicken Sie auf die **Übernehmen** Schaltfläche.

Die Einstellungen gelten für alle Geräte, auf denen die Sophos Mobile Security App installiert ist, in dem Kunden, an dem Sie angemeldet sind. Die in der Sophos Mobile Control Web-Konsole festgelegten Einstellungen können auf dem Endbenutzergerät nicht geändert werden. Sie sind ausgegraut.

Hinweis: Klicken der Schaltfläche **Liste der erlaubten Apps anzeigen** zeigt die Liste der erlaubten Apps an. Diese Liste kann aus der Liste der Scan-Ergebnisse von Geräten erstellt werden.

24.3 Definieren von Sophos Mobile Security Compliance-Einstellungen

Voraussetzung: Eine SMC Advanced-Lizenz ist verfügbar.

Sie können Compliance-Einstellungen, die sich auf Sophos Mobile Security beziehen, in der Web-Konsole konfigurieren.

1. Fügen Sie eine neue Geräterichtlinie hinzu oder öffnen Sie eine bereits vorhandene zum Bearbeiten. Weitere Informationen finden Sie unter Konfigurieren von Geräterichtlinien (Seite 35).
2. Wechseln Sie in die **Android** Registerkarte.
3. Im Feld **Max. SMSec-Scanintervall** können Sie das maximale Scanintervall zwischen Malware-Scans angeben, die von der Sophos Mobile Security App auf den Geräten durchgeführt werden.
4. Legen Sie im **Malware Apps zugelassen** Feld fest, ob auf Geräten gefundene Malware Apps zulässig sind.
5. Legen Sie im **Verdächtige Apps zugelassen** Feld fest, ob auf Geräten gefundene, verdächtige Apps zulässig sind.
6. Legen Sie im **PUA zugelassen** Feld fest, ob auf Geräten gefundene PUAs (Potentially Unwanted Apps) zulässig sind.
7. Wenn Sie alle erforderlichen Einstellungen konfiguriert haben, klicken Sie auf die **Speichern** Schaltfläche.

24.4 Einsehen von Sophos Mobile Security Scan-Ergebnissen

Voraussetzung: Eine SMC Advanced-Lizenz ist verfügbar.

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die **Geräte** Ansicht mit allen Geräten, die für diesen Kunden bei Sophos Mobile Control registriert sind, wird angezeigt.

2. Klicken Sie auf das blaue Dreieck neben dem gewünschten Gerät und dann auf **Bearbeiten** oder klicken Sie auf dessen Namen.

   Die **Gerät anzeigen** oder **Gerät bearbeiten** Ansicht wird angezeigt.

3. Wechseln Sie in die **Scan-Ergebnisse** Registerkarte.

   Diese Registerkarte zeigt die Sophos Mobile Security Scan-Ergebnisse. Die unsauberen Pakete, z. B. potenziell unerwünschte Anwendungen, werden in einer Tabelle darunter angezeigt. Unter **Threat-Name** können Sie auf die Links klicken, um weitere Informationen von SophosLabs zu den einzelnen Bedrohungen abzurufen.

4. Wechseln Sie in die **Richtlinienverletzungen** Registerkarte, um die mit den Scan-Ergebnissen verbundenen Compliance-Verletzungen einzusehen. Welche Verletzungen angezeigt werden, richtet sich nach den Sophos Mobile Security Compliance-Einstellungen.

24.4.1 Erstellen einer Liste erlaubter PUAs und Apps mit niedriger Reputation

Sie können die Scan-Ergebnisse verwenden, um eine Liste der erlaubten Apps zu erstellen. Die Liste gilt für alle Android-Geräte, auf denen die Sophos Mobile Security App installiert ist, in dem Kunden, an dem Sie angemeldet sind.

1. Wechseln Sie zur **Scan-Ergebnis** Registerkarte eines Ihrer gescannten Geräte.

   Die unsauberen Pakete werden in einer Tabelle angezeigt. Die Spalte **Threat-Name** zeigt an, ob das angezeigte Paket eine App niedriger Reputation, eine PUA oder Malware ist. Sie können auf die Links klicken, um weitere Informationen zur den einzelnen Bedrohungen von SophosLabs abzurufen.

   Gefundene Apps mit niedriger Reputation und PUAs haben ein blaues Häkchen-Symbol links vom Paketnamen. Nur diese Apps können zur Liste der erlaubten Apps hinzugefügt werden.

2. Klicken Sie auf das blaue Häkchen-Symbol, um die App zur Liste der erlaubten Apps hinzuzufügen.

   Ein Bestätigungsdialog wird angezeigt.

3. Klicken Sie auf **Ja**.

   Die App wird zur Liste der erlaubten Apps hinzugefügt.

4. Wiederholen Sie diesen Schritt für alle Apps, die Sie hinzufügen möchten.
5. Um die Liste anzuzeigen, gehen Sie auf **Einstellungen** und klicken Sie auf **Allgemein**.

6. Klicken Sie auf die Schaltfläche **Liste der erlaubten Apps anzeigen**.

   Alle Apps, die Sie hinzugefügt haben, werden angezeigt. Apps auf dieser Liste dürfen auf allen verwalteten Geräten gestartet werden. Die Apps werden in Zukunft nicht mehr gemeldet.

   Wenn Sie auf **Liste der erlaubten Apps löschen** klicken, dann werden alle Einträge in der Liste gelöscht.

25 Verwaltung von Sophos Secure Workspace über Sophos Mobile Control

Sophos Secure Workspace ist eine App für iOS und Android Mobiltelefone und Tablets, die Benutzern den Zugriff auf verschlüsselte Dateien, die in der Cloud gespeichert sind, ermöglicht. Dateien können nahtlos entschlüsselt und angezeigt werden. Verschlüsselte Dateien können von anderen Apps übergeben und zu einem der unterstützten Cloud Storage-Anbietern hochgeladen werden. Alternativ können die Dokumente lokal innerhalb der App gespeichert werden.

Mit Sophos Secure Workspace können Sie mit SafeGuard Cloud Storage oder SafeGuard Data Exchange verschlüsselte Dateien lesen. SafeGuard Cloud Storage und SafeGuard Data Exchange sind Module von SafeGuard Enterprise oder einer der verschiedenen Produkteditionen. Mit diesen Modulen lassen sich Dateien mit einem lokalen Schlüssel verschlüsseln. Diese lokalen Schlüssel werden aus einer Passphrase abgeleitet, die von einem Benutzer eingegeben wird. Sie können eine Datei nur dann entschlüsseln, wenn Sie die Passphrase kennen, mit der die Datei verschlüsselt wurde.

Die Sophos Secure Workspace Verwaltungsfunktion ist ein optionales Modul von Sophos Mobile Control. Zum Verwalten der Sophos Secure Workspace App über Sophos Mobile Control muss eine SMC Advanced-Lizenz verfügbar sein. Diese Lizenz muss in der Sophos Mobile Control Web-Konsole aktiviert werden.

So verwalten Sie die Sophos Secure Workspace App auf Managed-Geräten über die Sophos Mobile Control Web-Konsole:

- Sie können Einstellungen für die Sophos Secure Workspace App auf allen Managed-Endbenutzergeräten remote und zentral in der Web-Konsole konfigurieren.
- Sie können sicherstellen, dass die Sophos Secure Workspace App auf Endbenutzergeräten installiert ist. Sie können dies als Compliance-Kriterium definieren.
- Sie können die sichere Verteilung von Dokumenten aktivieren, indem Sie den Storage-Anbieter *Unternehmensdokumente* verwenden. Siehe Verteilen von Unternehmensdokumenten (Seite 113).

Hinweis: Zum Verwalten von Sophos Secure Workspace muss die App mit Sophos Mobile Control verteilt werden. Falls Benutzer bereits eine nicht verwaltete Version von Sophos Secure Workspace auf ihren Geräten installiert haben, müssen sie diese zunächst deinstallieren und danach die verwaltete Version installieren.

Weitere Informationen zu Sophos Secure Workspace finden Sie in der *Sophos Secure Workspace Hilfe*.

25.1 Konfigurieren von Sophos Secure Workspace

Voraussetzung: Eine SMC Advanced-Lizenz ist verfügbar.

Informationen zum Konfigurieren von Sophos Secure Workspace finden Sie unter **Mobile Encryption App** unter Verfügbare iOS-Konfigurationen (Seite 67) für iOS und Verfügbare Android-Konfigurationen (Seite 44) für Android.

25.2 Zurücksetzen des Kennworts für die Sophos Secure Workspace App

Sie können das Kennwort für die Sophos Secure Workspace App zurücksetzen. Das ist beispielsweise nützlich, wenn Benutzer ihr App-Kennwort vergessen haben. Wenn Sie ein App-Kennwort zurücksetzen, wird der Benutzer aufgefordert, ein neues App-Kennwort für Sophos Secure Workspace festzulegen.

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die **Geräte** Ansicht wird angezeigt.

2. Klicken Sie auf das Gerät, für das Sie das App Passwort zurücksetzen möchten.

   Die **Gerät anzeigen** Ansicht wird angezeigt.

3. Klicken Sie auf die **Aktionen** Schaltfläche.

   Das **Aktionen** Menü wird angezeigt.

4. Klicken Sie auf die Schaltfläche **App-Kennwort für SSW zurücksetzen**.

   Ein Bestätigungsdialog wird angezeigt.

5. Klicken Sie auf **Ja**.

Das Kennwort für Sophos Secure Workspace wird auf dem Gerät zurückgesetzt. Der Benutzer muss ein neues Kennwort für die Sophos Secure Workspace App eingeben.

25.3 Einrichten des Dokumentenzugriffs - Sophos Secure Workspace sperren und entsperren

Sie können Zugriffsrechte auf Dokumente einstellen, um Zugriff auf Unternehmensdaten in Sophos Secure Workspace zu verhindern. Wenn Sie **Dokumentenzugriff** auf **Sperren** setzen, kann Sophos Secure Workspace nicht verwendet werden.

1. Klicken Sie in der Web-Konsole unter **VERWALTEN** auf **Geräte**.

   Die **Geräte** Ansicht wird angezeigt.

2. Klicken Sie auf das Gerät, für das Sie den Dokumentenzugriff bearbeiten möchten.

   Die **Gerät anzeigen** Ansicht wird angezeigt.

3. Klicken Sie auf die **Aktionen** Schaltfläche.

   Das **Aktionen** Menü wird angezeigt.

4. Klicken Sie die **Dokumentenzugriff** Schaltfläche.

   Ein Dialog wird angezeigt, in dem Sie die Zugriffsrechte für Dokumente einrichten können.

5. Wählen Sie eine der folgenden Optionen:

   - **Sperren**, um Sophos Secure Workspace zu sperren. Die Benutzer können die Sophos Mobile Encryption App nicht mehr verwenden.
   - **Erlauben**, um Sophos Secure Workspace zu erlauben. Die Benutzer können die Sophos Mobile Encryption App weiterhin verwenden.

- **Automatischer Modus** um zu überprüfen, ob eine Richtlinienverletzung für dieses Gerät gemeldet wurde. Falls eine Richtlinienverletzung festgestellt wurde, wird Sophos Secure Workspace gesperrt.

6. Klicken Sie auf **Ja**.

Abhängig von Ihrer Auswahl wird Sophos Secure Workspace gesperrt oder erlaubt. Falls Sie die App gesperrt haben, wird ein Sperrbildschirm auf dem Gerät angezeigt, wenn Sophos Secure Workspace aktiviert wird. Benutzer haben keinen Zugriff auf Dokumente, die mit Sophos Secure Workspace gesichert wurden, solange Sie die App nicht entsperren.

26 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie die SophosTalk Community unter community.sophos.com/ auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support Knowledgebase unter http://www.sophos.com/de-de.aspx.
- Laden Sie die Produktdokumentation herunter unter www.sophos.com/de-de/support/documentation.aspx.
- Öffnen Sie ein Ticket bei unserem Support Team unterhttps://secure2.sophos.com/support/contact-support/support-query.aspx.

27 Rechtliche Hinweise

Copyright © 2011 - 2015 Sophos Ltd. Alle Rechte vorbehalten.

Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Sophos ist ein eingetragenes Warenzeichen von Sophos Limited. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.